Aprendendo Criptologia de Forma Divertida

Débora de Jesus Bezerra
Pedro Luiz Malagutti
Vânia Cristina da Silva Rodrigues

SUMÁRIO

Sepejampam bempem vinpindospos aopao
espestrapanhopo munpundopo dospos
cópódipigospos epe daspas cipifraspas!

1. INTRODUÇÃO

Enviar mensagens secretas é uma tarefa muito antiga. O homem sentiu, desde muito cedo, a necessidade de guardar informações em segredo; ela nasceu com a diplomacia e com as transações militares. Generais, reis e rainhas, durante milênios, buscavam formas eficientes de comunicação para comandar seus exércitos e governar seus países. A importância de não revelar segredos e estratégias às forças inimigas, motivou o desenvolvimento de códigos, cifras e técnicas para mascarar uma mensagem, possibilitando apenas ao destinatário ler o conteúdo.

As nações passaram a criar departamentos para elaborar sistemas criptográficos; por outro lado, surgiram os decifradores de códigos, criando uma corrida armamentista intelectual. Ao longo da história, os códigos decidiram o resultado de batalhas. À medida que a informação se torna cada vez mais valiosa, o processo de codificação de mensagens tem um papel cada vez maior na sociedade.

Tendo em vista a necessidade de se criar ferramentas capazes de proteger a informação e de prover segurança aos documentos armazenados e transmitidos pelas organizações através do mundo, tem-se a motivação para o estudo da Criptologia.

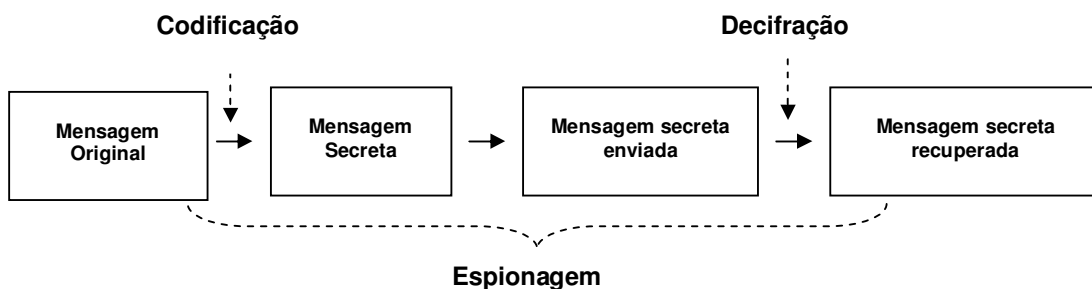
A Criptologia é a arte ou a ciência de escrever em cifra ou em código; em outras palavras, ela abarca o conjunto de técnicas que permitem tornar incompreensível uma mensagem originalmente escrita com clareza, de forma a permitir normalmente que apenas o destinatário a decifre e a compreenda.

Hoje em dia, entretanto, com o advento da comunicação eletrônica, a Criptografia deixou de ser unicamente segredo de estado, pois muitas atividades essenciais dependem do sigilo na troca de mensagens, principalmente aquelas que envolvem transações financeiras e uso seguro da Internet.

Até recentemente, a criptografia era considerada uma arte; hoje em dia, entretanto, passou a ser considerada uma ciência.

As aplicações da Criptografia atualmente incluem:

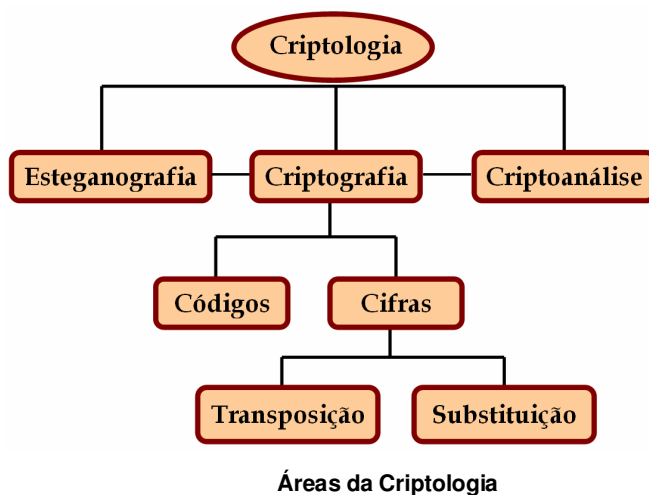
- sigilo em banco de dados;
- censos;
- investigações governamentais;
- dossiês de pessoas sob investigação;
- dados hospitalares;
- informações de crédito pessoal;
- decisões estratégicas empresariais;
- sigilo em comunicação de dados;
- comandos militares;
- mensagens diplomáticas;
- operações bancárias;
- comércio eletrônico;
- transações por troca de documentos eletrônicos (EDI);
- estudo de idiomas desconhecidos;
- recuperação de documentos arqueológicos, hieróglifos;
- e até tentativas de comunicações extraterrestres!

Simplificadamente, temos o seguinte diagrama:

Nosso objetivo neste mini-curso é apresentar atividades com criptografia através de aparatos que possam efetivamente ser construídos com materiais simples (papel, palito, clipe, furador de papel, cola e tesoura) para explorar alguns aspectos matemáticos destas construções. Os conteúdos matemáticos envolvidos são comumente estudados no Ensino Fundamental (1º. ao 9º. anos) e início do Ensino Médio.

2. ÁREAS DA CRIPTOLOGIA

A Criptologia é a ciência que se ocupa da ocultação de informações (criptografia) e da quebra das informações ocultadas (criptoanálise). Uma informação pode ser escondida de duas maneiras diferentes:

- Ocultando a existência da mensagem (esteganografia)
- Ocultando o significado do conteúdo da mensagem (criptografia propriamente dita)

Áreas da Criptologia

Esteganografia

A esteganografia estuda meios e métodos para se esconder a existência da mensagem. É bastante utilizada na área de segurança monetária, na autenticação de documentos, em imagens e nas gravações em geral (música, filmes, etc). Atualmente é utilizada na luta contra a pirataria e o terrorismo. Vejamos alguns exemplos:

A marca d´água (na figura, a bandeira nacional) é um recurso esteganográfico presente nas notas de dinheiro que ajuda a combater a falsificação.

A esteganografia em imagens digitais visa inserir dados dentro de uma imagem, através da manipulação dos bits (um **bit** é a menor parcela de informação processada por um computador; um bit comporta uma informação binária que somente pode assumir os valores 0 ou 1), de forma que ninguém note a existência de dados nesta imagem. Com as diversas possibilidades de envio e recepção de imagens digitais, e com a chegada da TV digital no Brasil, as técnicas de esteganografia em imagens digitais podem ser muito úteis no controle de cópias, uso e, entre outros, autoria das imagens. Veremos alguns usos desta técnica após estudarmos o sistema binário de numeração.

(Há números de 1 a 6 escondidos nas faces)

Criptografia

Para codificarmos ou decodificarmos uma mensagem necessitamos de informações confidenciais denominadas ***chave***. A ***criptoanálise*** estuda formas de decodificar uma mensagem sem se conhecer, de antemão, a chave. Ela reconstrói, a partir da mensagem codificada, a mensagem no seu formato original, com a ajuda de métodos matemáticos. Dizemos que a criptoanálise é responsável por quebrar o código da mensagem codificada, o que permite transformar dados ou mensagens em alguma forma legível.

A criptografia, por outro lado, é utilizada para proteger informações e manter o sigilo de dados confidenciais. A criptografia utiliza métodos para a produção e distribuição segura de chaves e estuda algoritmos que permitem transformar mensagens claras em formas de comunicação só inteligíveis pelos emissores e pelos receptores envolvidos no processo.

Apresentamos, a seguir, algumas definições usadas em Criptografia:

Criptograma: Mensagem cujo conteúdo foi obtido a partir de uma técnica de criptografia.

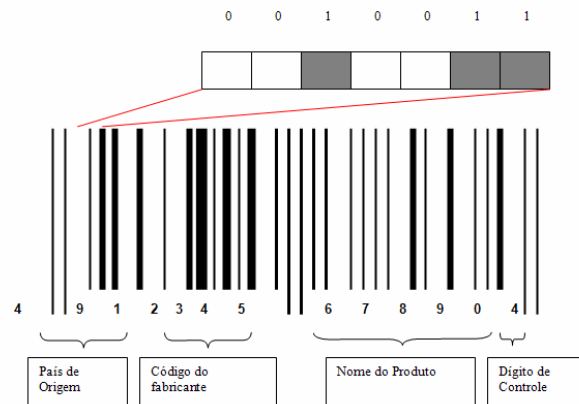
Ciframento: Técnica de criptografia para obter um criptograma a partir da mensagem.

Deciframento: Técnica de criptografia para obter a mensagem original a partir de um criptograma.

Na ciência da criptografia estudam-se os códigos e as cifras. No estudo de códigos em geral não há a intenção de se esconder a informação, como, por exemplo, nos códigos de barra, hoje em dia amplamente utilizados. Existem estudos matemáticos profundos sobre os códigos em geral (códigos corretores de erros, códigos baseados em teoria dos grupos ou em geometria algébrica, etc.).

Códigos

Códigos de Barras

Ultimamente todos os produtos vendidos em supermercados são identificados com códigos de barras, formados por uma seqüência alternada de linhas brancas e pretas. Nestas barras estão contidas informações sobre o fabricante, preço e origem. As barras pretas e brancas são convertidas, por meio de uma leitora ótica, em dígitos binários que podem ser entendidos pelo computador. Existem diferentes códigos de barras, mas o mais comum é constituído de no máximo 113 linhas. A linha preta corresponde ao binário 1 e a linha branca ao binário 0 e cada grupo de sete linhas representa um número que aparece imediatamente abaixo do código, mas não é em geral a representação binária deste número. Na verdade, as barras mais compridas têm a função apenas de separar as demais e as listras brancas e pretas que aparecem alternadamente podem ser de oito tipos: fina branca (0), média branca (00), grossa branca (000), muito grossa branca (0000), fina preta (1), média preta (11), grossa preta (111) e muito grossa preta (1111). Os códigos de barras de produtos produzidos no Brasil começam sempre com seqüência 789. A leitura deve ser feita em várias direções diferentes. Se você quiser mais informações sobre a matemática dos Códigos de Barra, principalmente sobre o papel do dígito de controle, acesse o trabalho de Polcino Milies no site: http://www.mat.ufg.br/bienal/2006/mini/polcino.pdf.

NÚMEROS DE CONTROLE

A Identidade de um Livro – ISBN

Todo livro recente tem um número que é sua identidade, o ISBN (*International Standard Book Number*): é um número que consiste 10 dígitos, indicados pelo editor. Por exemplo,

0 – 19 – 859617 – 0

é um número válido de um ISBN. Os hífens podem aparecer em diferentes lugares, isto não tem importância. O primeiro dígito da esquerda, 0, indica a linguagem utilizada no texto (no caso inglês); os próximos dois dígitos, 19, indicam a editora do livro (no caso *Oxford University Press*). Os próximos seis dígitos, 859617, formam propriamente o número do livro, sendo designado pelo editor. O último dígito é um número de controle. Ele é o que nos interessa. Com ele poderemos descobrir se o livro foi corretamente numerado e mesmo corrigir algum erro simples.

Para um ISBN da forma $x_1 – x_2\, x_3 – x_4\, x_5\, x_6\, x_7\, x_8\, x_9 - x_{10}$, o último dígito é calculado da seguinte forma: primeiro multiplicamos o número por sua posição e depois somamos os resultados. O que obtemos é:

$$1.\, x_1 + 2.\, x_2 + 3.\, x_3 + 4.\, x_4 + 5.\, x_5 + 6.\, x_6 + 7.\, x_7 + 8.\, x_8 + 9.\, x_9$$

A seguir, dividimos este número por 11 e tomamos o resto da divisão. Este será o valor de x_{10}. No exemplo que estamos considerando, o cálculo de x_{10} é feito da seguinte maneira:

$$1.\, 0 + 2.\, 1 + 3.\, 9 + 4.\, 8 + 5.\, 5 + 6.\, 9 + 7.\, 6 + 8.\, 1 + 9.\, 7 = 253.$$

Como 253 dividido por 11 resulta em resto 0, então $x_{10} = 0$. Se o resto for 10, devemos colocar a letra X no lugar de x_{10}.

Com este método de numerar livros, podemos detectar se algum erro simples foi feito ou se houve uma troca de posição de dois dígitos, estabelecendo assim uma espécie de controle, que evita erros simples de digitação. Como podemos fazer isto?

Efetuamos primeiramente a seguinte conta:

$$1.\, x_1 + 2.\, x_2 + 3.\, x_3 + 4.\, x_4 + 5.\, x_5 + 6.\, x_6 + 7.\, x_7 + 8.\, x_8 + 9.\, x_9 + 10\, .\, x_{10}.$$

e dividimos o resultado obtido por 11. Se o resto desta divisão não for igual a zero, o resultado está incorreto. De fato, mudar o valor de um dígito altera o valor do resto. Isto também acontece se ao escrevermos o número trocarmos a posição de dois dígitos, transpondo-os. Isto se deve ao fato de que todo número tem uma certa decomposição única, usando 11 como base do sistema de numeração.

Truque para adivinhar um número que está faltando no ISBN

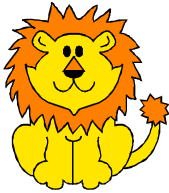
Se soubermos que apenas um número de um ISBN está ilegível, podemos recuperá-lo. Peça a alguém para escolher um livro não conhecido por você e ler o seu ISBN, mas dizendo “y” para um dos dígitos. Depois de fazer algumas continhas simples você poderá adivinhar o valor de y. Por exemplo, se o número for

0 – 20 – 11y – 502 – 7

calculamos

$$0.1+2.2+0.3+1.4+1.5+y.6+5.7+0.8+2.9+7.10 = 6.y+136$$

Como só nos interessa o resto da divisão do número por 11 e 136 = 11.12 + 4, precisamos encontrar y para que 6.y + 4 seja um múltiplo de 11. Basta testar e ver que y = 3 funciona. Logo, o número procurado é 3.

Como é feito o CPF (Cadastro de Pessoas Físicas)

O cadastro das pessoas físicas (usado nas declarações de imposto de renda) tem o seguinte formato:

$$X_1\ X_2\ X_3\ X_4\ X_5\ X_6\ X_7\ X_8\ R - C_1\ C_2$$

Os oito primeiros números constituem o número básico de inscrição da pessoa física no Cadastro Individual do Contribuinte.

O nono algarismo, indicado pela letra R, indica a região fiscal onde foi efetuada a inscrição. O dígito C_1 é um número verificador do número formado pelos nove algarismos anteriores (calculado tomando o resto por 11, como no ISBN) e C_2 é o dígito de controle que verifica a exatidão dos dez algarismos anteriores (usando também o resto por 11).

Cálculo de C_1: Cada um dos nove algarismos, a partir da direita é multiplicado sucessivamente por 2, 3, 4, 5, 6, 7, 8, 9, 10 e os produtos resultantes são somados. A soma obtida é então dividida por 11 e C_1 será o quanto falta para 11 do resto desta divisão. Se este complemento for maior ou igual a 10, toma-se o valor 0. Colocamos o valor encontrado de C_1 na sua devida posição para iniciar o cálculo de C_2.

Cálculo de C_2: Cada um dos dez algarismos, a partir da direita, é multiplicado sucessivamente por 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 e os produtos resultantes são somados. O número C_2 é obtido então de maneira análoga a C_1.

Exemplo: Vamos calcular os dígitos de controle C_1 e C_2 para o seguinte CPF:

1 2 3 4 5 6 7 8 5

Cálculo de C_1: 1.10+2.9+3.8+4.7+5.6+6.5+7.4+8.3+5.2 = 202. Dividindo 202 por 11, obteremos 4 como resto. Então $C_1 = 11 – 4 = 7$.

Cálculo de C_2: 1.11+2.10+3.9+4.8+5.7+6.6+7.5+8.4+5.3+7.2 = 257. Dividindo este número por 11, obteremos resto 4. Logo $C_2 = 11 - 4 = 7$.

Assim o CPF completo é: 123456785 – 77.

Como antes, se digitarmos ou escrevermos algum dígito errado, os dígitos de controle acusarão o erro, não é legal? É por isto que algumas máquinas recusam os CPFs digitados erroneamente.

Porque não vale a pena ser bagunceiro:

O algoritmo descrito acima para se calcular o CPF parece um tanto complicado, mas é baseado em regras rigorosas que nos permitem detectar erros. Podemos inventar muitos algoritmos para gerar e embaralhar números. O senso comum nos diz que quanto mais embaralhamos os números, mais confusos e aleatórios serão os resultados obtidos. Isto entretanto não é verdade. Vamos mostrar que do caos pode surgir a ordem e isto sem adentrar na Filosofia.

Considere o seguinte algoritmo gerador de números (devido a Donald Knuth):

0. Digite um número qualquer X com dez algarismos decimais.
1. Calcule Y = o algarismo mais significativo de X.
   As etapas 2 a 13 serão repetidas (Y + 1) vezes.
2. Calcule Z = o segundo algarismo mais significativo de X e vá para a etapa k(3+Z).
3. Se X < 5.000.000.000, some 5.000.000.000 a X.
4. Substitua X pelos 10 algarismos centrais de X^2.
5. Substitua X pelo resto da divisão de 1001001001X por 10.000.000.000
6. Se X < 1.000.000.000, some 98140556677 a X. Caso contrário, substitua X por 10.000.000.000 – X.
7. Troque os 5 algarismos menos significativos de X pelos 5 mais significativos e vice-versa (isto é o mesmo que substituir X pelos 10 algarismos centrais de 10.000.000.001X).
8. Repita a etapa 5.
9. Subtraia 1 de cada algarismo não nulo de X.
10. Se X < 100.000, substitua X por X^2 + 99.999. Caso contrário, subtraia 99.999 de X.
11. A instrução a seguir deve ser realizada duas vezes: Se X < 1.000.000.000, multiplique X por 10.
12. Substitua X pelos 10 algarismos centrais de X.(X-1).
13. Se Y > 0 (ver etapa 1), subtraia 1 de Y e volte à etapa 2. Caso contrário, termine.

Considerando todas as contorções do algoritmo acima, espera-se que ele deva produzir uma quantidade infinita de números aleatórios. Mas isto <u>não</u> acontece. Quando colocamos este algoritmo em um computador, ele converge, quase que imediatamente, para o número 6.065.038.420, o qual, é transformado nele mesmo pelo programa. Com outro número inicial, a seqüência começa a repetir-se após 7401 valores, num período cíclico de comprimento 3178.

Conclusão: mesmo para ser bagunceiro é preciso estudar muito.

Cifras

No estudo das cifras, o fundamental é o ocultamento da informação; há uma unidade básica de substituição formada por letras ou símbolos, isolados ou agrupados, e os métodos de cifragem são divididos segundo sua natureza: métodos de **substituição** (quando uma letra é trocada por outra, em geral diferente dela), cifragem de **transposição** (em que as letras da mensagem são apenas permutadas, mas não substituídas) e cifragem mista.

Vejamos com mais detalhes alguns destes métodos criptográficos.

Método de Ciframento por Transposição

Neste método os conteúdos das mensagens original e criptografada são os mesmos, porém com as letras são postas em ordem diferente (permutadas).

Exemplo: Pode-se cifrar a palavra CARRO e escrevê-la como ORARC. Mas cuidado! Não seja indelicado, ARGENTINO pode se transformar em IGNORANTE.

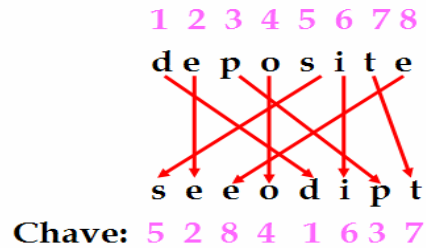
Exemplo – método da permutação de colunas: Dada a mensagem original,

deposite_um_milhão_de_dólares_em_minha
_conta_na_suiça._número_dois_um_sete_seis.

codifique a mensagem, utilizando o ciframento por transposição e a chave: 5 2 8 4 1 6 3 7.

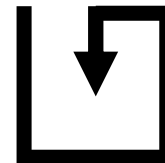
Divida a mensagem em bloco como exposto e aplique a chave dada em cada linha do bloco. O bloco é constituído de 8 colunas, que é o número de dígitos da chave. Devemos permutar as colunas de lugar de acordo com o indicado, isto é, a coluna 5 vira a primeira, a segunda fica onde está, a coluna 8 vira a terceira e assim sucessivamente .

d	e	p	o	s	i	t	e
_	u	m	_	m	i	l	h
ã	o	_	d	e	_	d	ó
l	a	r	e	s	_	e	m
_	m	i	n	h	a	_	c
o	n	t	a	_	n	a	_
s	u	i	ç	a	.	_	n
ú	m	e	r	o	_	d	o
i	s	_	u	m	_	s	e
t	e	_	s	e	i	s	.

Veja como fica a primeira linha criptogradada:

Se você utilizar um cartão com a tabela acima e recortar as colunas, será muito fácil cifrar ou decifrar a mensagem. Você pode também elaborar maneiras criativas de se lembrar da chave; por exemplo, a palavra FLORA serve para lembrar o número-chave 23451 se usarmos a ordem em que as letras aparecem no alfabeto.

No método da transposição ocorre apenas um embaralhamento das letras, dispostas em uma ordem pré-determinada para cifrar e decifrar.

Vejamos mais um exemplo: qual é o conteúdo da mensagem AASBMEROSATE? A resposta é simples se combinarmos a seguinte disposição:

A	A	S
B	M	E
R	O	S
A	T	E

Fácil, não?

A nossa mente é capaz de fazer coisas incríveis; leia as mensagens abaixo que andaram circulando pela Internet:

Como pode.... dá para ler tudo sem problema nenhum...rsrsrs

DE AORCDO COM UMA PQSIEUSA DE UMA UINRVESRIDDAE IGNLSEA, NÃO IPOMTRA EM QAUL ODREM AS LRTEAS DE UMA PLRAVAA ETÃSO, A ÚNCIA CSIOA IPROTMATNE É QUE A PIREMRIA E ÚTMLIA LRTEAS ETEJASM NO LGAUR CRTEO. O RSETO PDOE SER UMA TTAOL BÇGUANA QUE VCOÊ PDOE ANIDA LER SEM POBRLMEA. ITSO É POQRUE NÓS NÃO LMEOS CDAA LRTEA ISLADOA, MAS A PLRAVAA CMOO UM TDOO.

Observe bem, as letras não foram alteradas, apenas mudadas de ordem. Isto não ocorre, entretanto, na mensagem a seguir:

3M UM D14 D3 VER40, 3S7AVA N4 PR4I4,O853RV4NDO DU4S CR14NÇ4S 8B1NC4ND0 N4 4REI4. EL45 TR4B4LH4V4M MUI7O C0N57R1ND0 UM C4ATEL0 D3 AR3I4, C0M 70RR35, P4554R3L4S 3 P4554G3N5 1N7ERN4S. QU4ND0 ES74V4M QU4S3 T3RM1N4ND0, V310 UM4 0ND4 3 3S7RU1U 7UDO, R3DU21NDO 0 C4S7EL0 4 UM MON73 D3 4REI4 3 3SPUM4. 4CH31 QU3 D3P01S D3 74N70 35FORÇ0 3 CU1D4D0, 45 CR1ANC4S C4IR4M N0 CH0R0, CORR3R4M P3L4 PR41A, FUG1ND0 DA 4GU4, R1NDO D3 M405 D4D4S 3 C0M3C4R4M 4 C0NS7RU1R 0UTR0 C4573LO. C0NPR33ND1 QU3 H4V14 4PR3ND1D0 UM4 GR4ND3 L1Ç40; G4ST4M0S MU170 7EMP0 D4 NO554 V1D4 C0NS7RU1NDO 4LGUM4 C01S4 3 M41S 74RD3, UM4 0ND4 P0D3R4 V1R 3 DES7RU1R 7UD0 0 QU3 L3V4M0S 7ANTO 73MP0 P4R4 C0NS7RU1R.

Este último texto não é um exemplo de criptografia de transposição, mas sim de substituição, embora, convenhamos, de segurança mínima. Estudaremos os códigos de substituição na próxima seção.

A transposição e a substituição são frequentemente usadas como recursos poéticos. Vejamos algumas poesias concretas estes recursos[1]:

ZEN

[1] *Zen é uma poesia concreta de Pedro Xisto. Os dois outros poemas são de autoria de Augusto de Campos. Você reparou na mensagem escondida? Leia com calma a última poesia, explicitamente: colocar a máscara.*

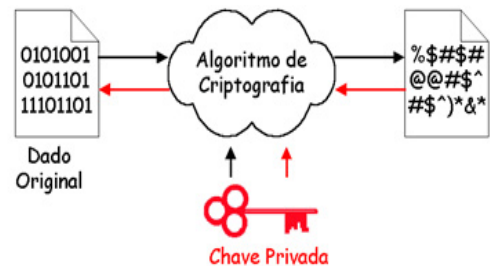
Método de Ciframento por Substituição

Neste procedimento troca-se cada letra ou grupo de letras da mensagem de acordo com uma tabela de substituição.

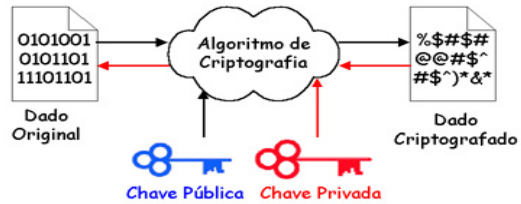
Exemplo: No método da substituição simples (monoalfabética) substitui-se cada caractere do texto por outro, de acordo com uma tabela pré-estabelecida. Por exemplo, na Segunda Guerra Mundial, era comum trocar cada letra pelo símbolo que estava acima do teclado da máquina de escrever. Vamos explorar vários destes sistemas nas atividades práticas da próxima seção.

Na criptografia contemporânea, com o uso de computadores, substitui-se caracteres por blocos de bits. Este método é relativamente seguro em textos muito curtos.

Classificação da Criptografia quanto às Chaves

Nos sistemas criptográficos ditos **simétricos** utiliza-se uma mesma chave secreta tanto para criptografar como para decifrar mensagens.

As teorias clássicas de criptografia são todas baseadas em chaves simétricas, isto é, a maneira de decifrar mensagens é praticamente a mesma que foi usada para cifrar.

Nos sistemas criptográficos ditos **assimétricos** utilizam-se duas chaves diferentes, que pertencem apenas a um participante. Uma é chamada chave pública e todos têm acesso a ela; a outra é secreta e deve ser guardada em sigilo.

Este sistema se assemelha ao que se usa em contas de banco; o número da conta-corrente é de conhecimento público, mas a senha pessoal só é conhecida pelo cliente.

Veremos na próxima seção um método chamado RSA, com chaves assimétricas, largamente em uso. O Algoritmo RSA (Rivest, Shamir, Adleman) foi descoberto em 1977 e se baseia em alguns princípios da Teoria dos Números; sua segurança se deve à dificuldade de fatorar números extensos, uma dificuldade tecnológica (por exemplo um número de 200 dígitos requer 4 bilhões de anos, supondo que o tempo de processamento de cada instrução é de 1 microssegundo).

Criframento misturando línguas

Uvi Strella

CHE scuitá strella, né meia strella!
Você stá maluco! e io ti diró intanto,
Chi p'ra iscuitalas montas veiz livanto,
i vô dá una spiada na gianella.

I passo as notte acunversáno c'oella,
Inguanto cha as otra lá d'un canto
St'o mi spiano. I o sol como um briglianto
Nasce. Ogliu p'ru çeu: _Cadê strella?!

Direis intó: _O' migno inlustre amigo!
O chi é chi as strallas tidizia
Quano illas viéro acunversá contigo?

E io ti diró: _Studi p'ra intendela,
Pois só chi giá studô Astrolomia,
É capaiz de intendê istas strella.

(Paródia de Juó Bananere)

Via Láctea

"Ora (direis) ouvir estrelas! Certo
Perdeste o senso"! E eu vos direi, no entanto,
Que, para ouvi-las, muita vez desperto
E abro as janelas, pálido de espanto...

E conversamos toda a noite, enquanto
A via láctea, como um pálio aberto,
Cintila. E, ao vir do sol, saudoso e em pranto,
Inda as procuro pelo céu deserto.

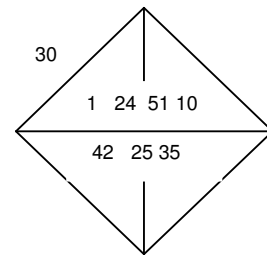
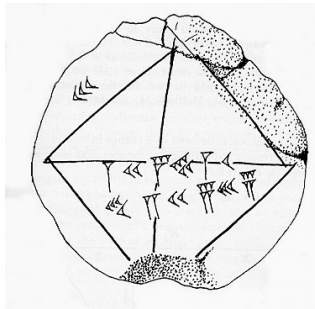
Direis agora! "Tresloucado amigo!
Que conversas com elas? Que sentido
Tem o que dizem, quando estão contigo?"

E eu vos direi: "Amai para entendê-las:
Pois só quem ama pode ter ouvido
Capaz de ouvir e de entender estrelas".

(Olavo Bilac)

3 HISTÓRIA DA CRIPTOLOGIA ATRAVÉS DE EXPERIMENTOS

ANTIGUIDADE (antes de 4000 a.C. a 476 d.C)

Todo código de comunicação envolve elementos criptográficos e, por isto, desde muito cedo o homem esteve às voltas com representações semióticas. Quando vistas com olhos de outras civilizações, parecem verdadeiros criptogramas. Observe por exemplo o objeto intitulado YBC 7289 (Yale Babylonian Collection):

Esta interessante peça arqueológica babilônica data de aproximadamente 1800 aC, traz o cálculo da raiz quadrada de 2 com sete casas decimais de precisão e está registrada em um tablete de argila com a escrita cuneiforme, como era uso na época. Apesar de seu interesse histórico e matemático ela não pode ser considerada uma verdadeiro achado criptográfico, pois não houve intenção de quem a escreveu de esconder a mensagem; pelo contrário, está claramente exposto o desejo de instruir a quem a lê, evidenciado pelos componentes geométricos nela gravados.

Também a Pedra de Roseta, decifrada por Campollion em 1822, não pode ser considerada um registro criptográfico; trata-se apenas de um texto escrito em três línguas: grego, egípicio demótico e com hieróglifos.

Na verdade os primeiros escritos verdadeiramente criptográficos aparecem em escritos religiosos, como veremos a seguir.

600 a 500 a.C.

Escribas hebreus, escrevendo o livro de Jeremias, usaram a cifra de substituição simples pelo alfabeto reverso conhecida como ATBASH. Eles não usavam vogais na sua escrita e metade das consoantes eram substituídas pela outra metade, ordenadamente, mas na ordem inversa. Isto fazia com que a letra a (aleph) ficasse codificada pela letra t (taw) e a letra b (beta) pela letra s (shin), daí o nome ATBASH.

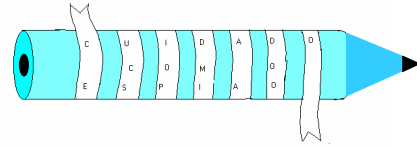
As cifras mais conhecidas da época são o ATBASH, o ALBAM e o ATBAH, as chamadas cifras hebraicas. Datam de 600-500 a.C. e eram usadas principalmente em textos religiosos. Estas cifras baseiam-se no sistema de substituição simples (monoalfabética). As três são denominadas reversíveis porque na primeira operação obtém-se o texto cifrado e, aplicando-se a mesma cifra ao texto cifrado, obtém-se o texto original. Este alfabeto foi usado para escrever parte dos rolos dos Escritos do Mar Morto.

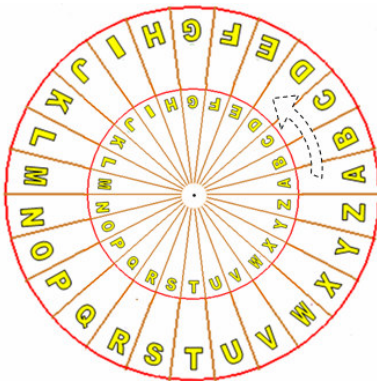
Diagrama do alfabeto hebreu

487 aC

Militares gregos desta época usavam o bastão de licurgo ou citale para enviar mensagens secretas.

Bastão de Licurgo

ATIVIDADE: Com dois lápis iguais e uma fita comprida de papel você pode facilmente construir este sistema criptográfico. Tente, veja se ele funciona e se é seguro.

A esteganografia também é antiga. A História registra que na Grécia Antiga um método utilizado baseava-se em raspar a cabelo de um escravo e tatuar uma mensagem em sua cabeça; quando o cabelo já estivesse grande o suficiente para esconder a mensagem, o escravo era enviado ao destinatário para que a mensagem pudesse ser entregue. É preciso, é claro, de muita paciência.

50 a. C.

Um dos primeiros sistemas de criptografia conhecido foi elaborado pelo general Júlio César, no Império Romano. Júlio César usou sua famosa cifra de substituição para encriptar comunicações governamentais. Para compor seu texto cifrado, César alterou letras desviando-as em três posições; A se tornava D, B se tornava E, etc. Às vezes, César reforçava sua encriptação substituindo letras latinas por gregas.

O código de César continua sendo usado até hoje. Atualmente denomina-se qualquer cifra baseada na substituição cíclica do alfabeto de código de César.

Vejamos com um exemplo com mais detalhes; como vimos, Júlio César substituiu cada letra, pela terceira letra que a segue no alfabeto.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Segundo este sistema, a palavra MATEMÁTICA passa a ser PDWHPDWLFD. Letras acentuadas não são levadas em conta.

ATIVIDADE: Cifre a mensagem abaixo usando o código de Júlio César: “SOCORRAM-ME SUBI NO ÔNIBUS EM MARROCOS”.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

ATIVIDADE: Decifre a mensagem:

OHJDO FRQVHJXL

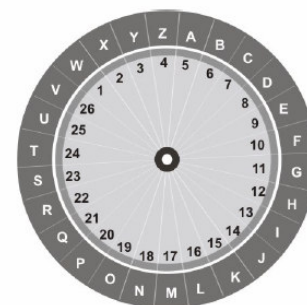
Ao invés de caminhar 3 letras para frente, podemos andar um outro número de letras e teremos um novo método de cifrar mensagens. Este número é a <u>chave</u> ou <u>senha</u> do sistema criptográfico; ele deve ser conhecido apenas por que envia a mensagem e por quem a recebe.

Podemos também transformar letras em números, segundo uma ordem pré-estabelecida. Por exemplo:

A=0	B=1	C=2	D=3	E=4	F=5	G=6	H=7
I=8	J=9	K=10	L=11	M=12	N=13	O=14	P=15
Q=16	R=17	S=18	T=19	U=20	V=21	W=22	X=23
Y=24	Z=25						

Deste modo a letra codificada é obtida da letra original, somando-se 3 ao número correspondente. E se o resultado ultrapassar 25? Caso isto ocorra, a letra codificada estará associada ao resto da divisão por 26 do número associado à letra original somado com 3. Por exemplo, a letra Y corresponde originalmente ao número 24, somando-se 3, obteremos 24 + 3 = 27 e, dividindo 27 por 26, obteremos resto 1 que corresponde à letra B. Assim Y deve ser codificado por B.

ATIVIDADE (OBMEP 2007)

(2) Um antigo método para codificar palavras consiste em escolher um número de 1 a 26, chamado *chave* do código, e girar o disco interno do aparelho ilustrado na figura até que essa chave corresponda à letra A. Depois disso, as letras da palavra são substituídas pelos números correspondentes, separados por tracinhos. Por exemplo, na figura ao lado a chave é 5 e a palavra *PAI* é codificada como 20-5-13.

(a) Usando a chave indicada na figura, descubra qual palavra foi codificada como 23-25-7-25-22-13.

(b) Codifique *OBMEP* usando a chave 20.

(c) Chicó codificou uma palavra de 4 letras com a chave 20, mas esqueceu-se de colocar os tracinhos e escreveu 2620138. Ajude o Chicó colocando os tracinhos que ele esqueceu e depois escreva a palavra que ele codificou.

(d) Em uma outra chave, a soma dos números que representam as letras *A*, *B* e *C* é 52. Qual é essa chave?

Se um espião conhecer a chave (a quantidade de letras que andamos), poderá facilmente decifrar uma mensagem interceptada, trocando cada letra pela terceira anterior. Mas, não se conhecendo a chave, como decifrar mensagens criptografadas? Pense um pouco a respeito disso. Nas próximas seções você aprenderá a decifrar facilmente as mensagens criptografadas no estilo Júlio César, mesmo desconhecendo inicialmente a chave. O método de decifração é baseado no estudo da **frequência das letras** de um determinado alfabeto.

Princípios de contagem em criptografia:

Nos sistemas que seguem o princípio do de Júlio César, podemos usar 25 chaves diferentes para obter codificações diferentes, já que o sistema com chave 0 (ou 26), não codifica nada. Nestes sistemas o alfabeto é codificado seguindo a <u>ordem</u> usual, apenas iniciando em um lugar diferente. Se, entretanto, pudermos alterar a ordem, obteremos um enorme número de maneiras de criptografar. Vejamos alguns exemplos:

a) Alfabeto quebrado ao meio:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M

b) Troca de dois vizinhos:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	A	D	C	F	E	H	G	J	I	L	K	N	M	P	O	R	Q	T	S	V	U	X	W	Z	Y

Observe que nenhuma letra ficou no seu lugar original. Neste caso, dizemos que houve um **desordenamento**.

c) Usando a seqüência que aparece no teclado do computador:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Q	W	E	R	T	Y	U	I	O	P	A	S	D	F	G	H	J	K	L	Z	X	C	V	B	N	M

Aqui também houve desordenamento.

Atividade: Usando o código:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

Decifre a mensagem:

Z TIZNZ V' ZNZITZ

Leia de trás para frente a mensagem decifrada.

Quantas maneiras diferentes de criptografar podemos construir?

Digamos que em um planeta distante os alfabetos fossem formados por apenas três símbolos: ⌂, □ e ◊. Poderíamos criptografar mensagens de seis maneiras diferentes:

1 ⌂	2 □	3 ◊
1 ⌂	2 □	3 ◊

1 ⌂	2 □	3 ◊
3 ◊	1 ⌂	2 □

1 ⌂	2 □	3 ◊
2 □	3 ◊	1 ⌂

1 ⌂	2 □	3 ◊
1 ⌂	3 ◊	2 □

1 ⌂	2 □	3 ◊
3 ◊	2 □	1 ⌂

1 ⌂	2 □	3 ◊
2 □	1 ⌂	3 ◊

A primeira dessas maneiras é a "trivial" e não serve para codificar nada. Sem listar as mensagens, poderíamos concluir que existem seis maneiras diferentes de permutar as letras deste alfabeto? É claro que sim: para a primeira letra existem 3 possibilidades de codificação, para a segunda apenas duas e para a terceira resta somente uma possibilidade.

O Princípio Multiplicativo da Contagem:
Se uma decisão puder ser tomada de *m* maneiras diferentes e se, uma vez tomada esta primeira decisão, outra decisão puder ser tomada de *n* maneiras diferentes, então, no total serão tomadas *mxn* decisões.

Pelo **Princípio Multiplicativo da Contagem**, são

$$3 \,.\, 2 \,.\, 1 = 6$$

as possibilidades. Há uma notação muito útil para se trabalhar como produtos do tipo acima, camada **fatorial**. Por exemplo, o fatorial de 3 é 3! = 3.2.1. No caso geral, para um inteiro positivo n, define-se $n! = n.(n-1).(n-2).\ ...\ .3.2.1$ e, por convenção, 0! =1.

Observe que dentre estas, são três as possibilidades que mantém a "ordem usual" ⌂ → □ → ◊ → ⌂ (1→2→3→1) inalterada:

Quantos desordenamentos há neste caso? Apenas dois:

Digamos que em um outro planeta são quatro as letras empregadas: ⌂, □, ◊ e ○. Há, neste caso, 4 . 3 . 2. 1 = 4! = 24 maneiras diferentes de permutar as "letras". Dentre estas, apenas 4 respeitam a ordem usual ⌂ → □ → ◊ → ○ → ⌂. São elas:

Há 9 desordenamentos:

O que ocorre se usarmos as 26 letras de nosso alfabeto? Podemos inferir algo?

Existem 26! maneiras diferentes de criptografar, isto dá

403 291 461 126 605 635 584 000 000

possibilidades! Se, entretanto, quisermos preservar a ordem usual das letras, temos somente 26 maneiras, incluindo a trivial em que cada letra é trocada por ela mesma.

Em geral, se tivermos *n* letras, teremos *n! = n . (n-1) . (n-2).   . 3. 2.1* permutações diferentes e somente *n* delas respeitam a ordem usual. É possível também calcular os desordenamentos (em que nenhuma letra fica no seu lugar natural). O número total de desordeamentos com *n* letras é:

$$n!(\frac{1}{0!}-\frac{1}{1!}+\frac{1}{2!}-\frac{1}{3!}+...+\frac{(-1)^n}{n!})$$

(para ver a dedução desta fórmula veja o livro *Análise Combinatória e Probabilidade* de Morgado, Pitombeira de Carvalho, Pinto Carvalho e Fernandez – IMPA, 1991).

Como curiosidade, com 26 letras o número de desordenamentos é: 148 362 637 348 470 135 821 287 825.

Com tantas possibilidades de codificação, parece extremamente difícil descobrir a chave para se quebrar um código no estilo de Júlio César, caso desconheçamos qual foi a maneira com que as letras foram inicialmente codificadas, não é mesmo? Não há esperança alguma de se testar todas as possibilidades. Apesar disto o código de Júlio César e suas variações são muito fáceis de ser quebradas, como veremos a seguir.

Como quebrar o código de Júlio César

MAPAS DE TESOUROS

Vamos ilustrar a teoria da decifração com um trecho de um conto do escritor Edgar Allan Poe, intitulado “O Escaravelho de Ouro” [2]. O personagem principal desta obra, em uma certa altura da obra, encontra um velho pergaminho que acredita ser um mapa de um tesouro, com os seguintes dizeres:

[2] Este conto faz parte do livro “*História de Mistério e Imaginação*” de Edgar Allan Poe, Editorial Verbo, nº. 15, Lisboa.

(53±±+305))6; 4826) 4±.)4±);806*;48+8π
60))85;1±(;:±*8+83(88)5*+;46(;88*96*?;8)*±(;485);5*+2:*±(;4956* 2 (5*-4)8π8* ;
4069285);)6+8)4±±;1(±9;48081 ; 8:8±1;48+85;4) 485 + 528806* 81(±9;48; (88;4 (± ? 34;48) 4 ±
; 161 ; : 188; ±?;*

No conto, após uma análise baseada na frequência das letras do alfabeto inglês feita pelo protagonista, a mensagem toma a seguinte forma:

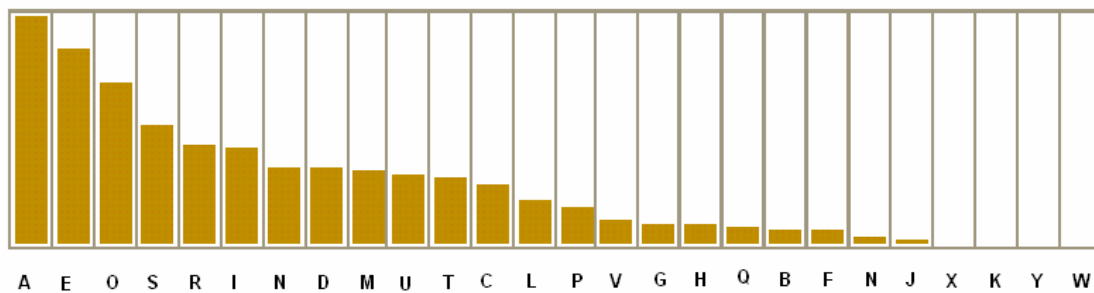
A good glass in the bishop's hostel in the devil's seat forty-one degrees and thirteen minutes north-east and by north main branch seventh limb east side shoot from the left eye of the death's-head a bee line form the tree through the shot fifty feet out.

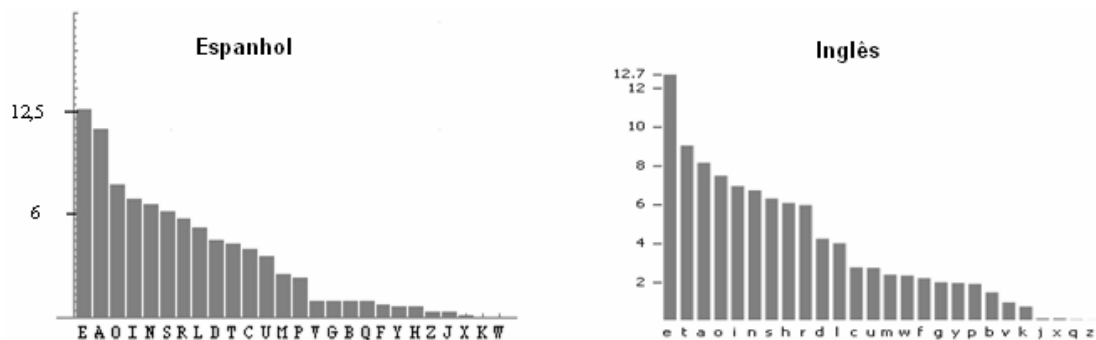
Como isto foi obtido? A letra que aparece com mais freqüência na língua inglesa é a letra e; muitas vezes ela aparece dobrada ee. Na mensagem secreta acima o símbolo 8 aparece 33 vezes, muito mais do que as outras letras e portanto é plausível que 8 deva significar a letra e. Substituindo 8 por e, e tentando o mesmo esquema com outras letras é possível decifrar a mensagem. Sua tradução para o português é:

Um bom vidro na hospedaria do bispo na cadeira do diabo quarenta e um graus e treze minutos nordeste e quarta de norte ramo principal sétimo galho do lado leste a bala através do olho esquerdo da cabeça do morto uma linha de abelha da árvore através da bala cinqüenta pés para fora.

O conto então revela, de uma maneira fantástica, como, a partir destas informações, o personagem principal encontra um tesouro há muito tempo enterrado por um pirata que passou pelo lugar descrito na mensagem.

O estudo da frequência das letras do alfabeto constitui um método eficaz para se quebrar mensagens no estilo de Júlio César.

Frequência aproximada das letras em português:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14,6	1,0	3,8	4,9	12,5	1,0	1,3	1,2	6,1	0,4	0,02	2,7	4,7	5,0	10,7	2,5	1,2	6,5	7,8	4,3	4,6	1,6	0,01	0,2	0,01	0,4

Como curiosidade, veja como aproximadamente se distribuem as letras no espanhol e no inglês:

Para contrariar a regra, seria possível escrever um texto longo sem a letra a? Você consegue, certo? (Esta frase "Você consegue, certo?" não tem a letra a), tente construir um texto com pelo menos 5 linhas.

Atividade: Usando as frequências das letras em português, decifre a mensagem abaixo e complete a tabela para registrar as substituições encontradas.

Urtklm tr dqapuakcftr ltr iasqtr aj nmqsuouar lacfdqa t jakrtoaj tetfxm a cmjniasa t steait ntqt qaofrsqtq tr ruersfsufcmar akcmksqtltr.

Sugestão:Vamos observar a frequência das letras na frase.

Observe na tabela as ocorrências:

Letra	Número de vezes que aparece na frase	Letra	Número de vezes que aparece na frase
t	18	l	4
a	16	j	4
r	13	n	3
q	9	i	3
s	8	o	3
u	6	e	3
m	6	d	1
f	6	p	1
k	5	x	1
c	5		

Como a frequência de letras em português segue a ordem; A E O R S I N ...., muito provavelmente a letra t deve ser a codificação da letra A, pois é a mais frequente, assim como a letra a deve ser a codificação da letra E, que é a segunda mais freqüente, mas isto, por enquanto, é só uma especulação.

Se substituirmos t por A e a por E na mensagem criptografada, chegaremos a

UrAklm Ar dqEpuEkcfAr lAr iEsqAr Ej nmqsuouEr lEcfdqE A jEkrAoEj AeAfxm E cmjniEsE A sAeEiA nAqA qEofrsqAq Ar ruersfsufcmEr EkcmksqAlAr.

Será que já conseguimos descobrir o que está escrito? Vamos analisar a terceira letra mais frequente; a letra r que aparece 13 vezes na frase. Ela pode estar codificando as seguintes letras ou O ou R ou S.

Se r codificar O a mensagem fica:
UOAklm AO dqEpuEkcfAO lAO iEsqAO Ej nmqsuouEO lEcfdqE A jEkOAoEj AeAfxm E cmjniEsE A sAeEiA nAqA qEofOsqAq AO OueOsfsufcmEO EkcmksqAlAO.

Se r codificar R a mensagem fica:
URAklm AR dqEpuEkcfAR lAR iEsqAR Ej nmqsuouER lEcfdqE A jEkRAoEj AeAfxm E cmjniEsE A sAeEiA nAqA qEofRsqAq AR RueRsfsufcmER EkcmksqAlAR.

Se r codificar S a mensagem fica:
USAklm AS dqEpuEkcfAS lAS iEsqAS Ej nmqsuouES lEcfdqE A jEkSAoEj AeAfxm E cmjniEsE A sAeEiA nAqA qEofSsqAq AS SueSsfsufcmES EkcmksqAlAS.

Das três opções acima a mais provável é a terceira, pois muitas palavras terminam em S.
A quarta letra a ser analisada é a letra q. Provavelmente ela é a codificação da letra O ou da letra R.

Se for da letra O, a mensagem fica:

USAklm AS dOEpuEkcfAS lAS iEsOAS Ej nmOsuouES lEcfdOE A jEkSAoEj AeAfxm E cmjniEsE A sAeEiA **nAOA** OEofSsOAO AS SueSsfsufcmES EkcmksOAlAS.

(observe a palavra nAOA em negrito, ela corresponde a alguma palavra em português?). É melhor ficar com a segunda opção em que a letra q corresponde à letra R:

USAklm AS dREpuEkcfAS lAS iEsRAS **Ej** nmRsuouES lEcfdRE A jEkSAoEj AeAfxm E cmjniEsE A sAeEiA nARA REofSsRAR AS SueSsfsufcmES EkcmksRAlAS.

A palavra Ej em negrito é uma pista de que a letra j deve ser a codificação da letra m. Se for a mensagem se transforma em:

USAklm AS dREpuEkcfAS lAS iEsRAS EM nmRsuouES lEcfdRE A **MEkSAoEM** AeAfxm E cmMniEsE A sAeEiA nARA REofSsRAR AS SueSsfsufcmES EkcmksRAlAS.

A palavra MEkSAoEM deve ser a codificação de MENSAGEM. Logo k corresponde à letra N e o corresponde à letra G. Fazendo essas substituições:

USANlm AS dREpuENcfAS lAS iEsRAS EM nmRsuGuES **lEcfdRE** A MENSAGEM AeAfxm E cmMniEsE A sAeEiA nARA **REGfSsRAR** AS SueSsfsufcmES ENcmNsRAlAS.

Podemos reconhecer as palavras em negrito: lEcfdRE deve ser DECIFRE e REGfSsRAR deve ser REGISTRAR. Se assim for, l é D, c é C mesmo, f é I, d é F e s é T. Fazendo estas substituições:

USANDm AS FREpuENCIAS DAS iETRAS EM nmRTuGuES DECIFRE A MENSAGEM AeAIxm E CmMniETE A TAeEiA nARA REGISTRAR AS SueSTITuICmES ENCmNTRADAS.

É possível decifrar agora? Se você não conseguir, volte e releia o enunciado da atividade.

Se você achou trabalhoso decifrar a mensagem da Atividade acima, saiba que existem vários *softwares* que fazem esta tarefa brincando. Veja por exemplo os *sites*: http://demonstrations.wolfram.com/CipherEncoder/ e http://demonstrations.wolfram.com/LetterHighlightingInText/

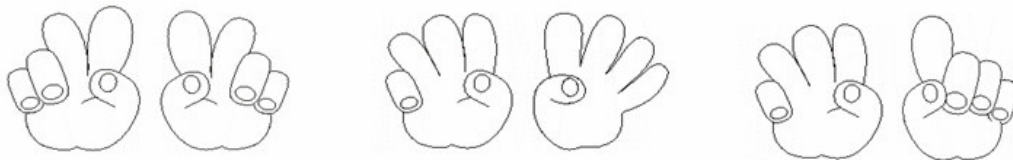
Variações:

1) Uma maneira de encriptar mensagens consiste em escolher uma palavra chave que deve ser mantida em segredo por quem as envia e por quem as recebe. Esta palavra não deve ter letras repetidas. Por exemplo, consideramos a palavra TECLADO. Para fazer a troca de letras, podemos usar a seguinte correspondência:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
T	**E**	**C**	**L**	**A**	**D**	**O**	B	F	G	H	I	J	K	M	N	P	Q	R	S	U	V	W	X	Y	Z

2) Outra maneira para codificar mensagens é feita trocando-se letras por números, de acordo com a seguinte tabela:

	1	**2**	**3**	**4**	**5**
1	**A**	**B**	**C**	**D**	**E**
2	**F**	**G**	**H**	**I/J**	**K**
3	**L**	**M**	**N**	**O**	**P**
4	**Q**	**R**	**S**	**T**	**U**
5	**V**	**W**	**X**	**Y**	**Z**

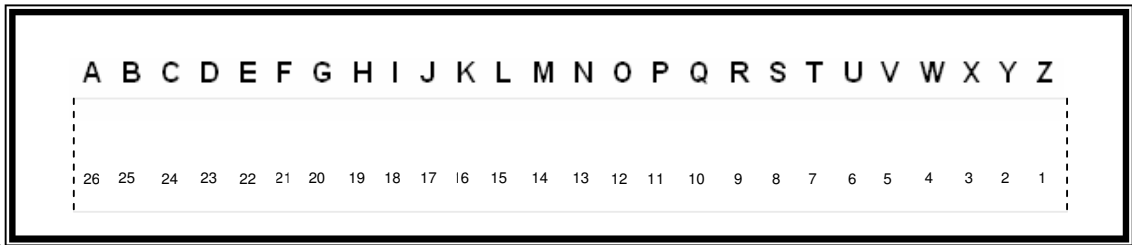
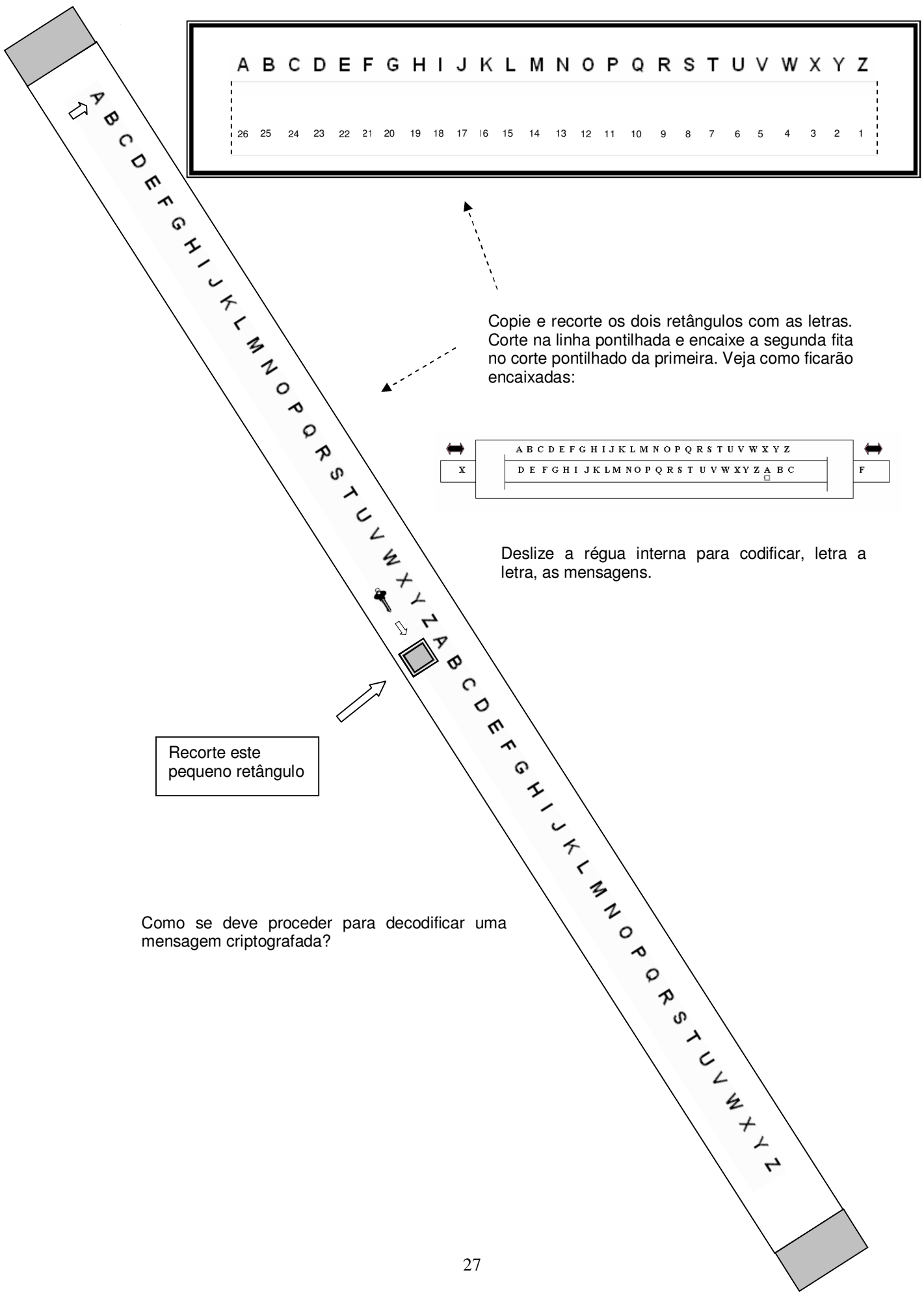
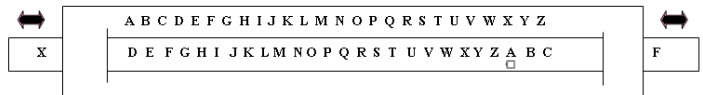
Por exemplo, a palavra LEGAL pode ser codificada como 31-15-22-11-31. Este código pode ser transmitido com as mãos: os dedos da mão direita indicam as linhas e os da esquerda as colunas. O que dizem as mãozinhas abaixo?

Construção de aparatos que ajudam a criptografar no estilo de Júlio César.

Vamos apresentar quatro aparatos simples para agilizar a criptografia no estilo de Júlio César:

- as réguas deslizantes,
- o quadrado de Vigenère[3],
- dois projetos: a lata de criptografar e o CD para criptografar.

Como veremos, são todos variações simples de um mesmo tema.

Atividade: Copie, recorte e monte as réguas deslizantes, conforme as instruções na página seguinte.

[3] Blaise Vigenère foi um diplomata francês, estudioso de Criptografia, que viveu no século XVI.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
26 25 24 23 22 21 20 19 18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1
Copie e recorte os dois retângulos com as letras. Corte na linha pontilhada e encaixe a segunda fita no corte pontilhado da primeira. Veja como ficarão encaixadas:
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
X
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
F
Deslize a régua interna para codificar, letra a letra, as mensagens.
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Recorte este pequeno retângulo
Como se deve proceder para decodificar uma mensagem criptografada?

As diferentes posições que a régua deslizante ocupa quando movimentada podem ser simultaneamente visualizadas no quadrado de Vigenère:

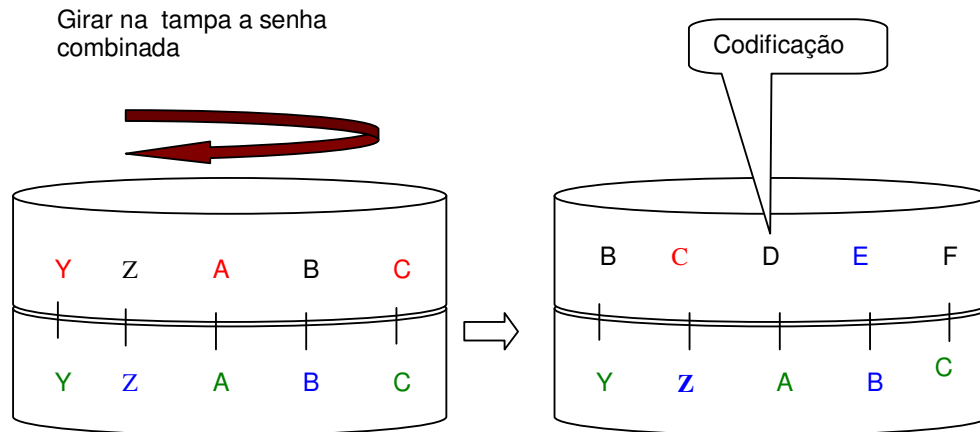
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Atividade: Utilizando a régua deslizante ou o quadrado de Vigenère, decifre a mensagem:

UHV JVUZLNBP KLJPMYHY UHKH

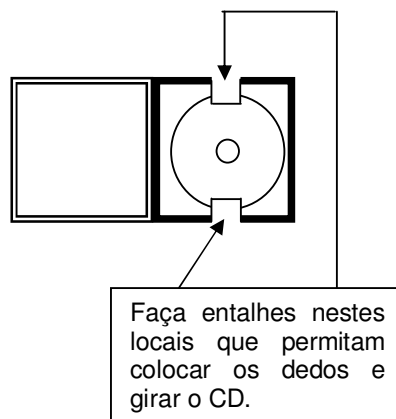
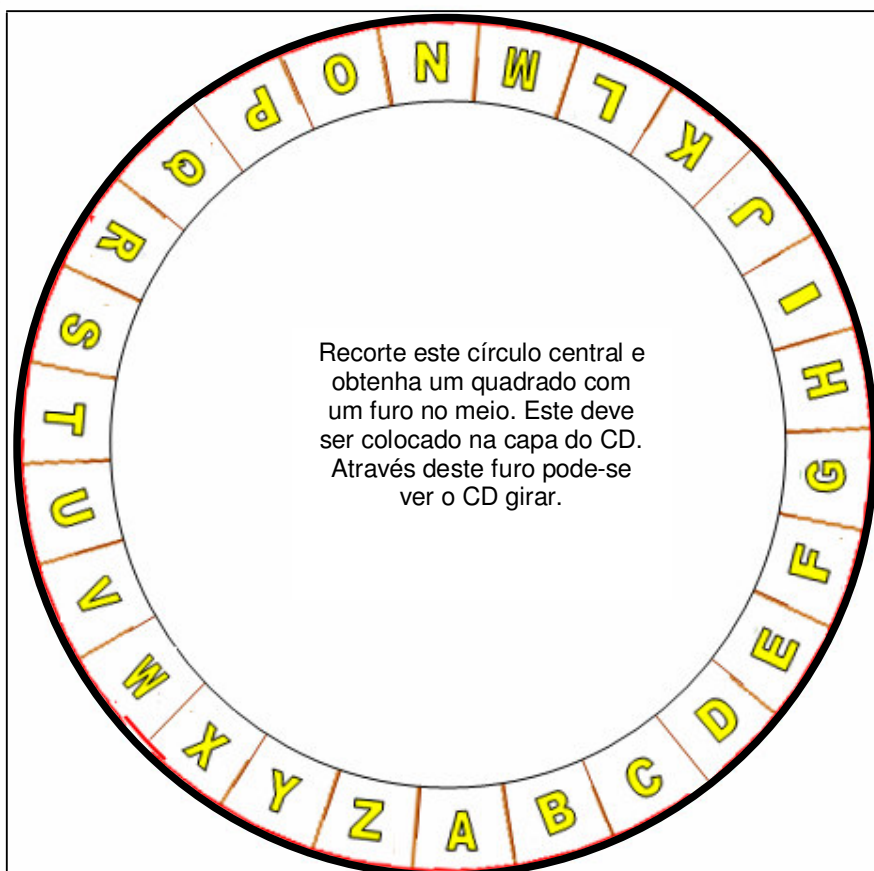
Como você fez para descobrir a chave?

Atividade: Projetos práticos de criptografia no estilo de Júlio César

LATA DE CRIPTOGRAFAR

CD PARA CRIPTOGRAFAR:

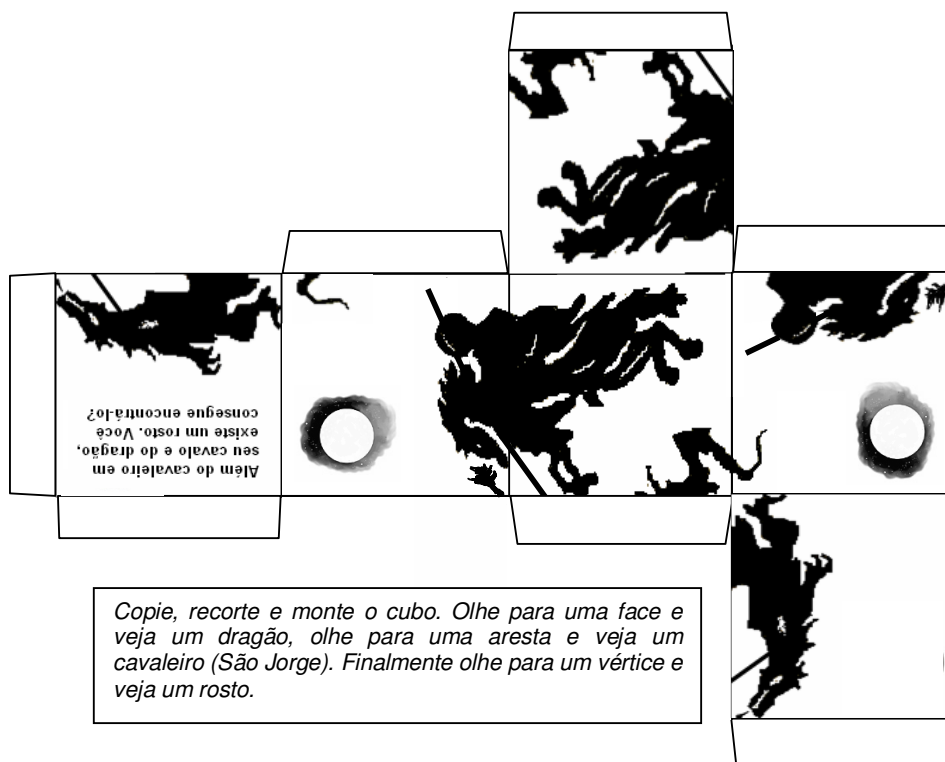
Para confeccionar este aparato você vai precisar de um CD que não tenha mais uso e também de sua caixinha.

Reproduza e recorte o círculo e cole-o no CD. O CD deve ser encaixado dentro da caixinha.

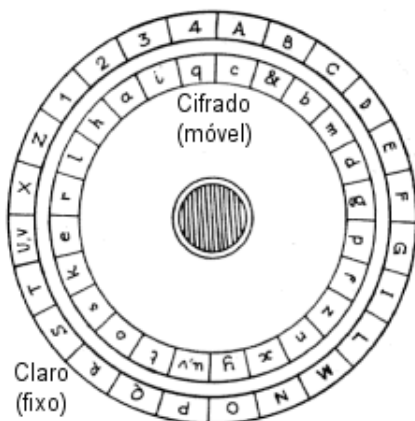
O quadrado com o furo no meio deve ser colocado na capa do CD. Para fazer a máquina funcionar você deve recortar na parte detrás da caixinha dois pequenos retângulos, suficientes para introduzir os dedos e girar o CD.

CÍRCULO PARA CRIPTOGRAFAR
Recorte este círculo e cole em um CD que já foi descartado. Encaixe o CD na posição usual dentro da caixinha.
N M L K J I H G F E D C B A Z Y X W V U T S R Q P O
Recorte este círculo central e obtenha um quadrado com um furo no meio. Este deve ser colocado na capa do CD. Através deste furo pode-se ver o CD girar.
N M L K J I H G F E D C B A Z Y X W V U T S R Q P O

IDADE MÉDIA (476 a 1453)

Na Europa, o período inicial desta época também foi chamado de "período das trevas", e a criptologia não escapou desta "recessão". Muito do conhecimento sobre o assunto foi perdido porque era considerado magia negra ou bruxaria. Nesta época, a contribuição árabe-islâmica foi significativa, principalmente com o desenvolvimento da criptanálise para a substituição monoalfabética. A denominação "Cifra", "Chiffre", "Ziffer", etc, como também "zero", utilizado em muitas línguas, vem da palavra árabe "sifr", que significa "nulo".

A Itália foi a primeira a acordar, iniciando o movimento renascentista ao redor de 1300, sendo responsável pelos primeiros grandes avanços. Veneza criou uma organização especializada em 1452, cujo único objetivo era lidar com a criptologia. Foram criadas três secretarias que solucionavam e criavam cifras usadas pelo governo da época.

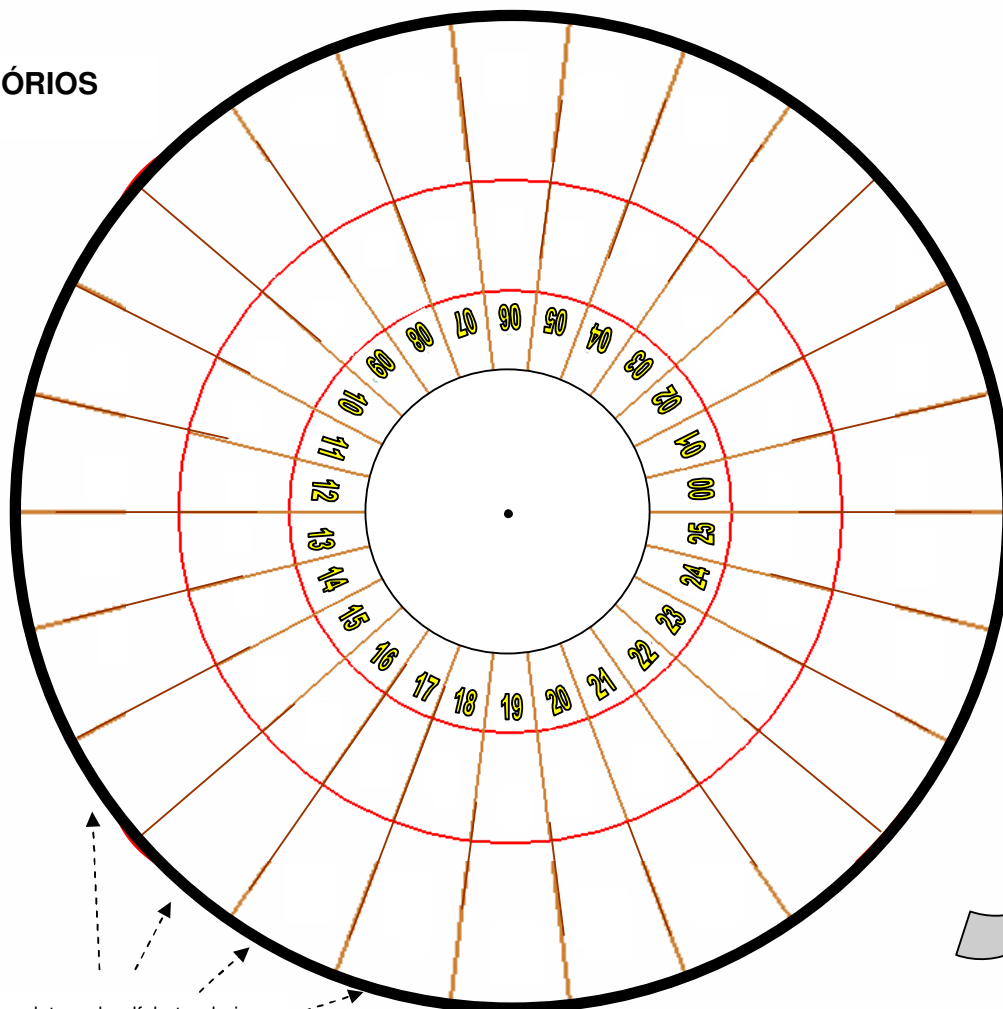
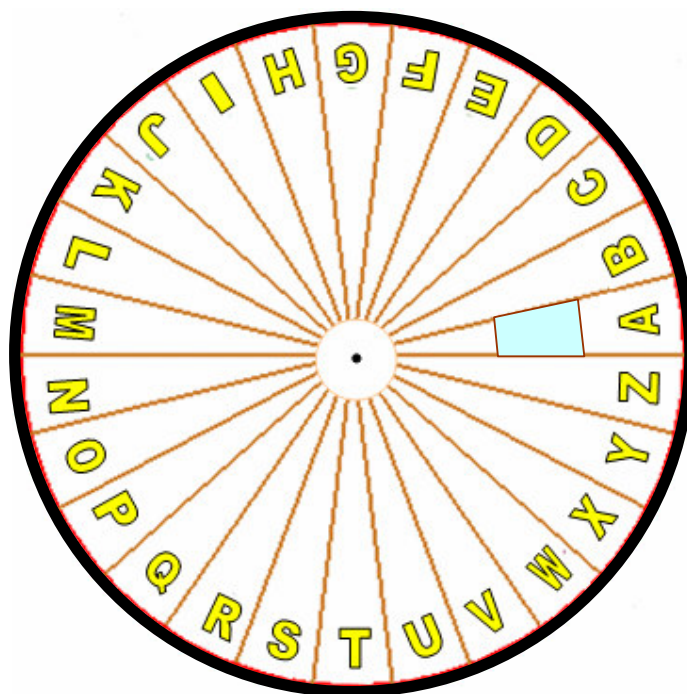
Copie, recorte e monte o cubo. Olhe para uma face e veja um dragão, olhe para uma aresta e veja um cavaleiro (São Jorge). Finalmente olhe para um vértice e veja um rosto.

IDADE MODERNA (1453 a 1789)

1466

Leon Battista Alberti (1404-1472) é conhecido como "o pai da criptologia ocidental", em parte porque desenvolveu a substituição polialfabética. A substituição polialfabética é uma técnica que permite que diferentes símbolos cifrados possam representar o mesmo símbolo do texto claro. Isto dificulta a interpretação do texto cifrado pela aplicação da análise de frequência dos símbolos. Para desenvolver esta técnica, Alberti estudou os métodos para quebrar cifras da época e elaborou uma cifra que não podia ser quebrada por eles. Ele criou um disco de cifragem para simplificar o processo. Introduziu a técnica de recifragem na criptografia.

Alberti sugeriu o uso de um disco composto por dois anéis concêntricos: um externo, fixo, com 24 casas contendo 20 letras latinas maiúsculas (incluindo o Z, com U=V e excluindo H J K W Y) mais os números 1, 2, 3, e 4 para o texto claro; e um interno, móvel, com as 24 letras latinas minúsculas para o texto cifrado. Nestes discos, as 20 letras maiúsculas estão em ordem alfabética e as 24 minúsculas estão fora de ordem. Colocar as letras minúsculas fora de ordem é fundamental pois, caso estivessem em ordem, a cifra seria apenas uma generalização do Código de César. Ao que tudo indica, os códigos inventados por Alberti não foram quebrados até os anos de 1800.

Atividade: Copie, recorte e monte os discos giratórios, conforme as instruções da próxima página. Nos espaços vazios complete cada um deles com uma letra diferente à sua escolha para que você tenha sua maneira de criptografar.

DISCOS GIRATÓRIOS

Copie e recorte o disco maior e o disco menor. Copie e recorte também o pequeno trapézio do círculo menor, formando uma janelinha. Sobreponha os dois discos. Coloque um palito de dentes ou um clipe perfurando os centros dos discos para que um deles gire com relação ao outro.

Copie e recorte as letras do alfabeto abaixo, embaralhe-as e cole-as uma a uma nos espaços vazios do círculo maior.

1563

O físico italiano Giambattista Della Porta (1535?-1615) foi o inventor do primeiro sistema literal de chave dupla, ou seja, a primeira cifra na qual o alfabeto cifrante muda a cada letra. Della Porta inventou seu sistema em 1563 e esta cifra foi utilizada com sucesso por mais de três séculos.

Vejamos qual foi a inovação introduzida por Della Porta: preenchemos primeiramente uma tabela com 26 x 26 = 676 símbolos diferentes à nossa escolha e em qualquer ordem. Vamos utilizar os números naturais em sua ordem usual como um exemplo, mas, para dificultar a criptoanálise, devemos usar símbolos não convencionais, ordenados aleatoriamente.

LITERAE SCRIPTI

LITERAE CLAVIS

A B	a	b	c	d	e	f	g	h	i	l	m
	n	o	p	q	r	s	t	v	x	y	z
C D	a	b	c	d	e	f	g	h	i	l	m
	z	n	o	p	q	r	s	t	v	x	y
E F	a	b	c	d	e	f	g	h	i	l	m
	y	z	n	o	p	q	r	s	t	v	x
G H	a	b	c	d	e	f	g	h	i	l	m
	x	y	z	n	o	p	q	r	s	t	v
I L	a	b	c	d	e	f	g	h	i	l	m
	v	x	y	z	n	o	p	q	r	s	t
M N	a	b	c	d	e	f	g	h	i	l	m
	t	v	x	y	z	n	o	p	q	r	s
O P	a	b	c	d	e	f	g	h	i	l	m
	s	t	v	x	y	z	n	o	p	q	r
Q R	a	b	c	d	e	f	g	h	i	l	m
	r	s	t	v	x	y	z	n	o	p	q
S T	a	b	c	d	e	f	g	h	i	l	m
	q	r	s	t	v	x	y	z	n	o	p
V X	a	b	c	d	e	f	g	h	i	l	m
	p	q	r	s	t	v	x	y	z	n	o
Y Z	a	b	c	d	e	f	g	h	i	l	m
	o	p	q	r	s	t	v	x	y	z	n

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
B	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52
C	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78
D	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100	101	102	103	104
E	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127	128	129	130
F	131	132	133	134	135	136	137	138	139	140	141	142	142	144	145	146	147	148	149	150	151	152	153	154	155	156
G	157	158	159	160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182
H	183	184	185	186	187	188	189	190	191	192	193	194	195	196	197	198	199	200	201	201	203	204	205	206	207	208
I	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223	224	225	226	227	228	229	230	231	232	233	234
J	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255	256	257	258	259	260
K	261	262	263	264	265	266	267	268	269	270	271	272	273	274	275	276	277	278	279	280	281	282	283	284	285	286
L	287	288	289	290	291	292	293	294	295	296	297	298	299	300	301	302	303	304	305	306	307	308	309	310	311	312
M	313	314	315	316	317	318	319	320	321	322	323	324	325	326	327	328	329	330	331	332	333	334	335	336	337	338
N	339	340	341	342	343	344	345	346	347	348	349	350	351	352	353	354	355	356	357	358	359	360	361	362	363	364
O	365	366	367	368	369	370	371	372	373	374	375	376	377	378	379	380	381	382	383	384	385	386	387	388	389	390
P	391	392	393	394	395	396	397	398	399	400	401	402	403	404	405	406	407	408	409	410	411	412	413	414	415	416
Q	417	418	419	420	421	412	423	424	425	426	427	428	429	430	431	432	433	434	435	436	437	438	439	440	441	442
R	443	444	445	446	447	448	449	454	451	452	453	454	455	456	457	458	459	460	461	462	463	464	465	466	467	468
S	469	470	471	472	473	474	475	476	477	478	479	480	481	482	483	484	485	486	487	488	489	490	491	492	493	494
T	495	496	497	498	499	500	501	502	503	504	505	506	507	508	509	510	511	512	513	514	515	516	517	518	519	520
U	521	522	523	524	525	526	527	528	529	530	531	532	533	534	535	536	537	538	539	540	541	542	543	544	545	546
V	547	548	549	550	551	552	553	554	555	556	557	558	559	560	561	562	563	564	565	566	567	568	569	570	571	572
W	573	574	575	576	577	578	579	580	581	582	583	584	585	586	587	588	589	590	591	592	593	594	595	596	597	598
X	599	600	601	602	603	604	605	606	607	608	609	610	611	612	613	614	615	616	617	618	619	620	621	622	623	624
Y	625	626	627	628	629	630	631	632	633	634	635	636	637	638	639	640	641	642	643	644	645	646	647	648	648	650
Z	651	652	653	654	655	656	657	658	659	660	661	662	663	664	665	666	667	668	669	670	671	672	673	674	675	676

Para criptografar, dividimos a palavra em pares de letras e procuramos o valor de cada par na tabela. Por exemplo, a palavra PATA, fica dividida como

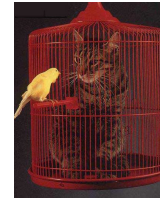
PA-TA e no encontro da linha P com a coluna A temos o número 391 e na linha T com a coluna O temos o número 495. Logo PATA fica codificada como 391-495. Observe que a repetição da letra A na palavra PATA não fica explícita na substituição por números. Para decifrar é só procurar na tabela os números correspondentes e montar as palavras, lembrando que em cada par a letra da linha é a primeira, seguida pela letra da coluna. Ou seja o procedimento é simétrico.

Desta época datam os quadros de Giuseppe Arcimboldo (1527?-1593?); os objetos e animais escondem rostos que representam os quatro elementos da natureza: terra, fogo, ar e água. Aprecie os recursos esteganográficos de sua obra:

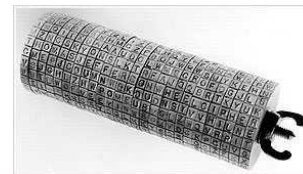
Até mesmo o filósofo inglês Francis Bacon (1561-1626) se aventurou por códigos criptográficos. Na verdade ele inventou um código criptoesteganográfico bastante interessante: a partir de um texto suporte qualquer, sem codificação alguma, usam-se dois caracteres ligeiramente diferentes. Usaremos exageradamente maiúsculas e minúsculas, só para mostrar como funciona o método. Cada grupo de 5 letras do texto suporte representa uma única letra do texto que queremos criptografar. Para fixar as ideias, digamos que as minúsculas valem 0 e as maiúsculas valem 1. Usamos então um método simples de substituição, trocando letras por sequências de cinco zeros ou uns. Por exemplo, usando-se a tabela de substituição

A	**11000**	B	10011	C	01110	D	10010	E	10000	F	10110	**G**	**01011**
H	00101	I	01100	J	11010	K	11110	L	01001	M	00111	N	00110
O	**00011**	P	01101	Q	11101	R	01010	S	10100	**T**	**00001**	U	11100
V	01111	W	11001	X	10111	Y	10101	Z	10001				

a palavra GATO pode ser codificada usando-se o texto “Um passarinho na gaiola”:

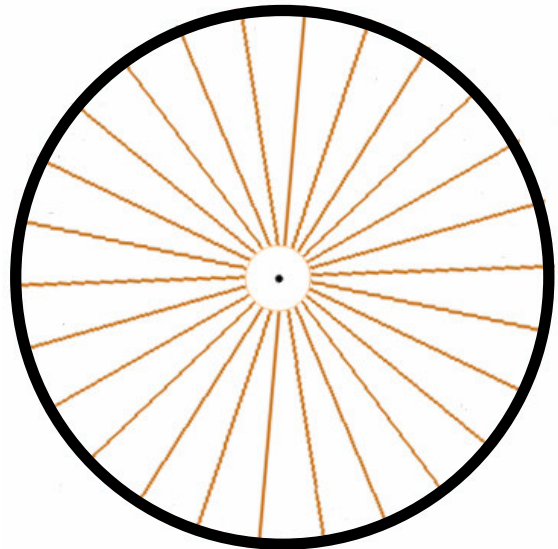
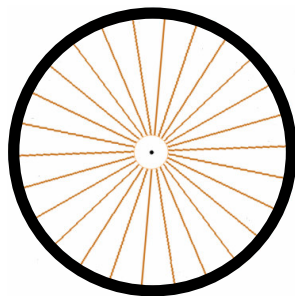
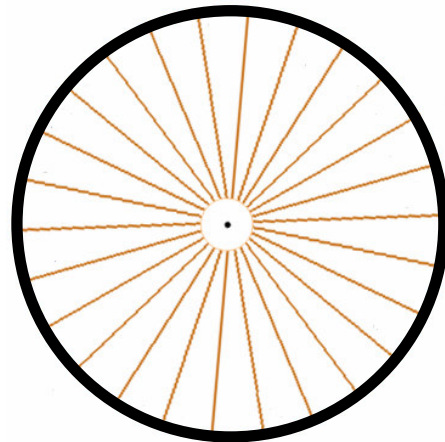
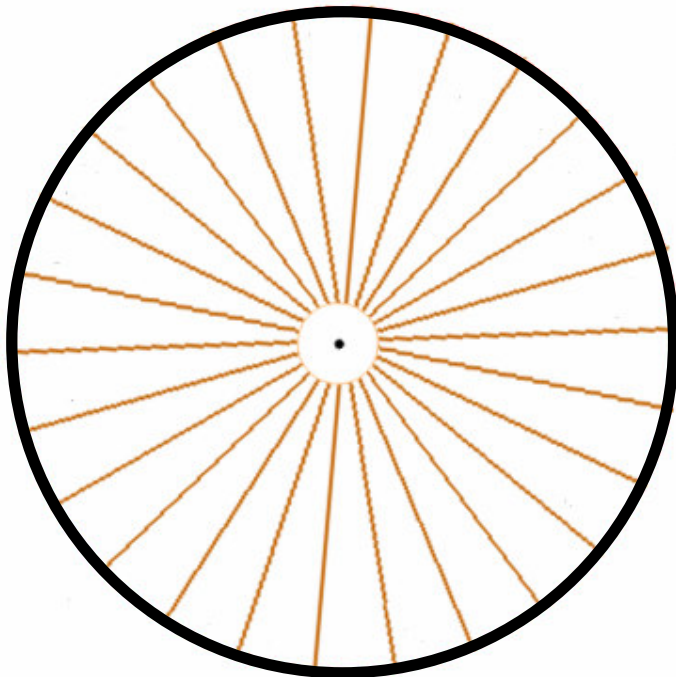
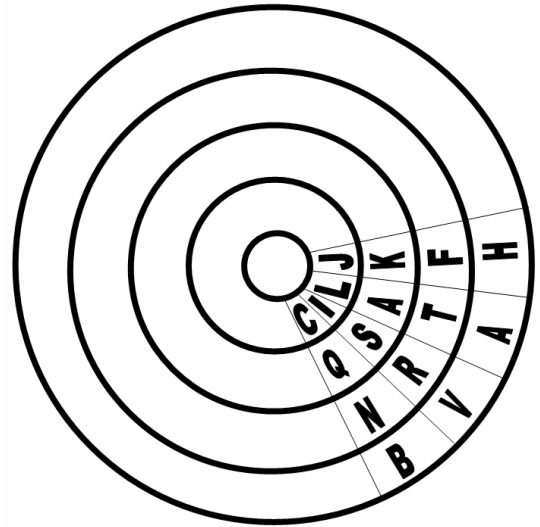
uMpAS	SArin	honaG	aioLA
01011	11000	00001	00011
G	A	T	O

HISTÓRIA RECENTE (1790 a 1900)

1795

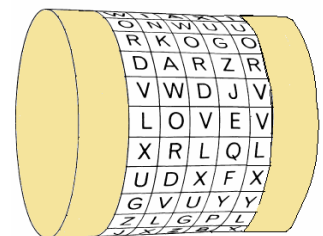
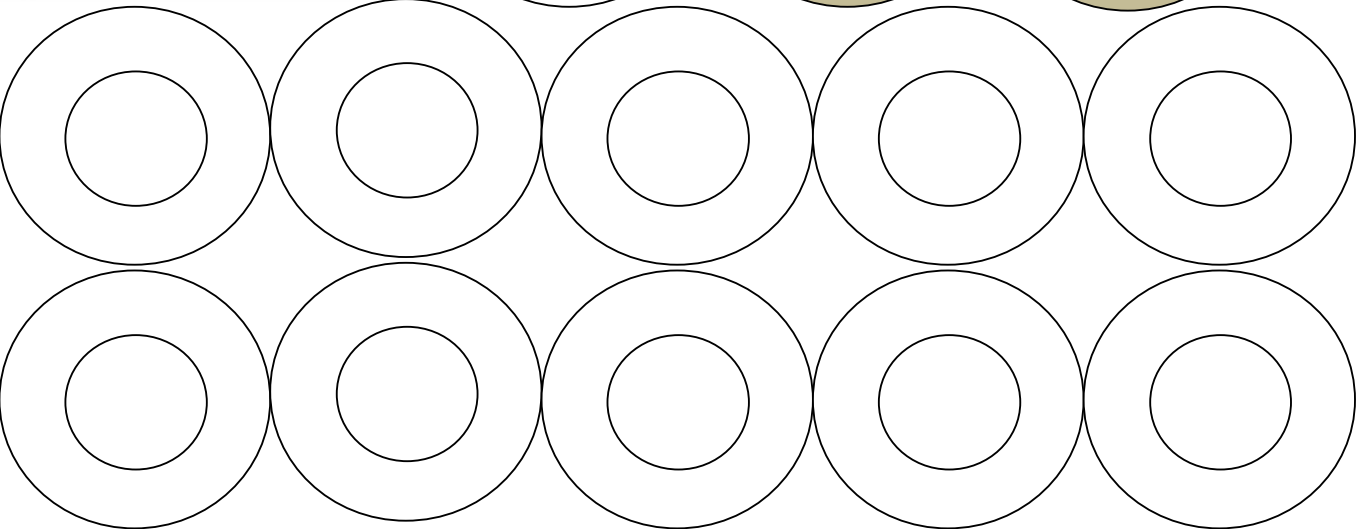
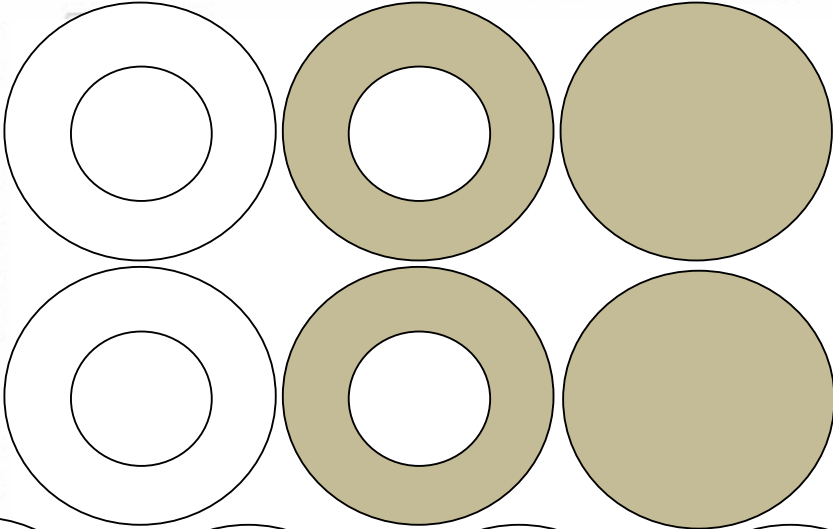
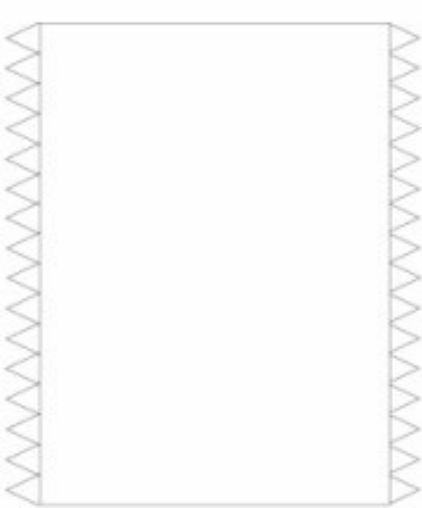
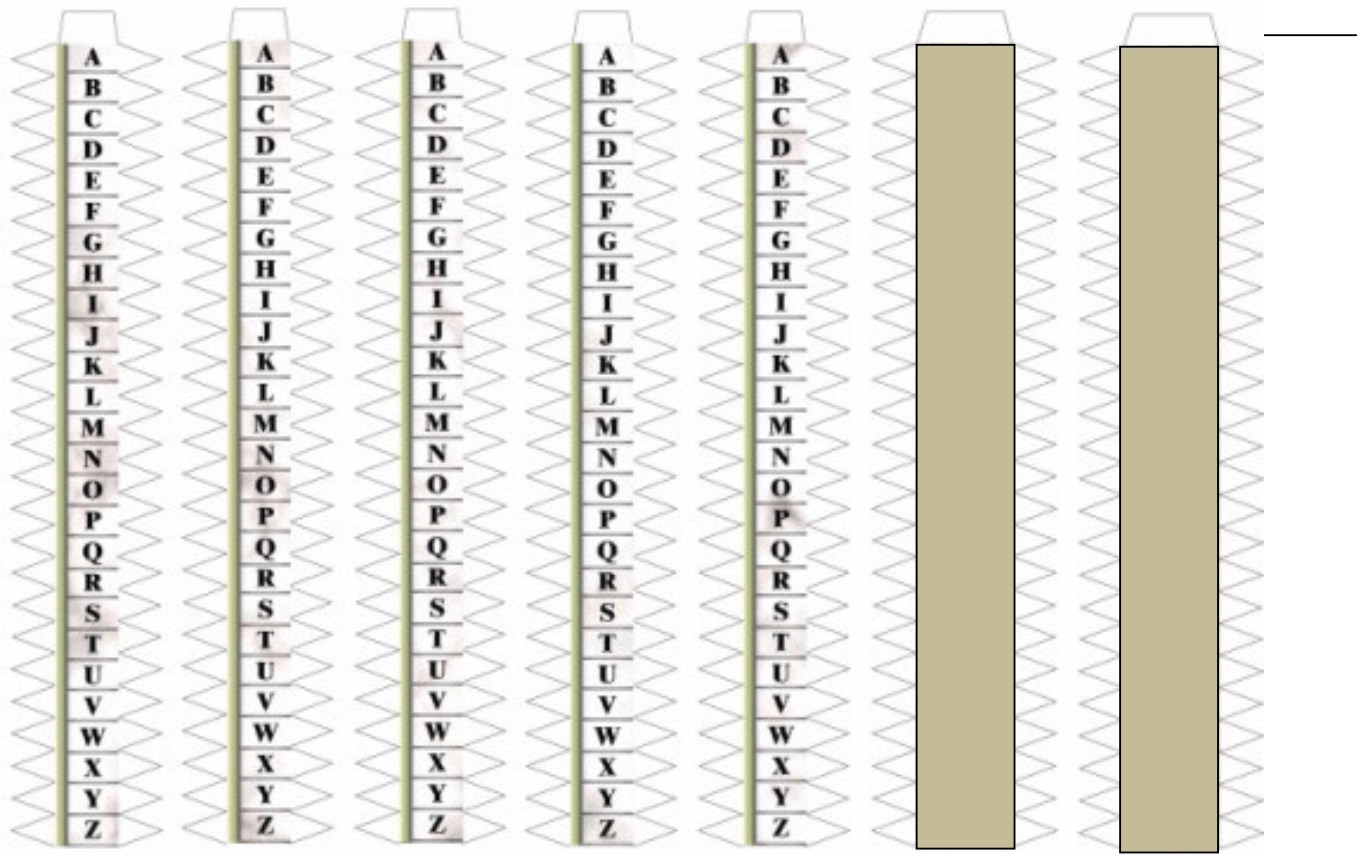
Na época em que era secretário de estado de George Washington, Thomas Jefferson (1743-1826), futuro presidente dos Estados Unidos, criou um método simples, engenhoso e seguro de crifrar e decifrar mensagens: o cilindro cifrante. Durante a revolução americana, Jefferson confiava cartas importantes a mensageiros que as entregavam pessoalmente. Porém, quando se tornou ministro americano para a França, os códigos assumiram grande importância na sua correspondência porque os agentes de correio europeus abriam e liam todas as cartas que passavam pelos seus comandos. Apesar de, aparentemente, Jefferson ter abandonado o uso do cilindro cifrante em 1802, ele foi reinventado um pouco antes da Primeira Guerra Mundial e foi usado pelo exército americano e outros serviços militares. O cilindro de Jefferson, na sua forma original, é composto por 26 discos de madeira que giram livremente ao redor de um eixo central de metal. As vinte e seis letras do alfabeto são inscritas aleatoriamente na parte mais externa de cada disco de modo que, cada um deles, possuía uma sequência diferente de letras. Girando-se os discos pode-se obter as mensagens.

Veremos como construir um cilindro análogo ao de Thomas Jefferson. Há também um cadeado cifrante, conhecido como Cryptex, que usa o mesmo princípio (invenção de Dan Brown em *O Código Da Vinci)*.

CRIPTOGRAFIA COM MÚLTIPLOS CÍRCULOS

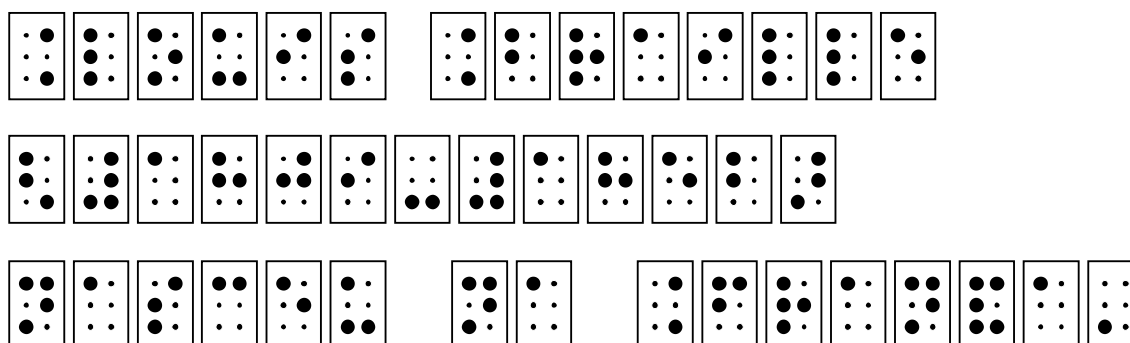
(*estilo Thomas Jefferson)*

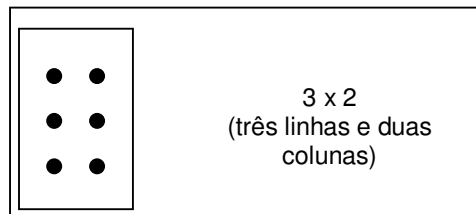
- É necessário ter dois conjuntos idênticos de círculos concêntricos (com 4 círculos cada). Use os quatro círculos abaixo como modelo.
- Preencha os dois conjuntos de círculos de modo idêntico, distribuindo como quiser as 26 letras do alfabeto em cada círculo.
- No exemplo, a mensagem clara é **LATA**
- O texto criptografado pode ser qualquer outro alinhamento, por exemplo **ISRV**
- Os outros alinhamentos, em geral, não têm significado
- Quem recebe, alinha **ISRV** e procura nos outros alinhamentos palavras que façam sentido
- Para textos longos, fazemos a divisão das letras em blocos de 4.

CILINDRO DE JEFFERSON DE PAPEL

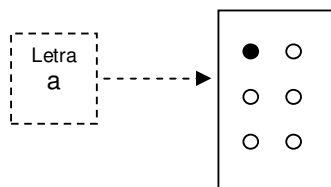
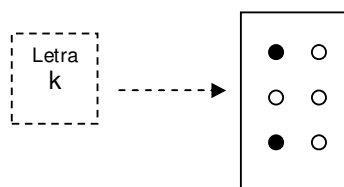
Copie e recorte as peças da folha seguinte e com eles monte um cilindro de criptografar no estilo Jefferson.

A
B
C
D
E
F
G
H
I
J
K
L
M
N
O
P
Q
R
S
T
U
V
W
X
Y
Z

1834

Louis Braille (1809-1852), educador francês, ficou cego aos 3 anos de idade. Interessou-se por um sistema de escrita, apresentado na escola Charles Barbier, no qual uma mensagem codificada em pontos era cunhada em papel-cartão. Aos 15 anos de idade trabalhou numa adaptação, escrita com um instrumento simples. O Código Braille consiste de 63 caracteres, cada um deles constituído por 1 a 6 pontos dispostos numa matriz ou célula de seis posições. Mais tarde adaptou este sistema para a notação musical. Publicou tratados sobre seu sistema em 1829 e 1837. O Sistema Braille é universalmente aceito e utilizado até os dias de hoje.

Você consegue ler a seguinte mensagem?

Louis Braille ficou cego devido a um ferimento no olho feito com um objeto pontiagudo que seu pai usava para fabricar selas de animais; o ferimento infeccionou e isto provocou também a perda da visão no outro olho, deixando-o com deficiência visual total.

Como dissemos, o código Braille é baseado em um arranjo 3 x 2 de pontos, dispostos como nas pedras de um dominó:

Para registrar uma dada letra do alfabeto, alguns desses 6 pontos são marcados ou perfurados, de modo a se tornarem sobressalentes, para que possam ser sentidos com as pontas dos dedos das mãos.

Quando um ponto estiver marcado, usaremos um círculo negro e, quando não estiver, um círculo branco. Veja os exemplos:

Somente a primeira casa foi marcada: o ponto que está na primeira linha e na primeira coluna aparece em negro.

A letra k tem marcas pretas em dois pontos: o ponto da primeira linha e da primeira coluna e o ponto da terceira linha e primeira coluna.

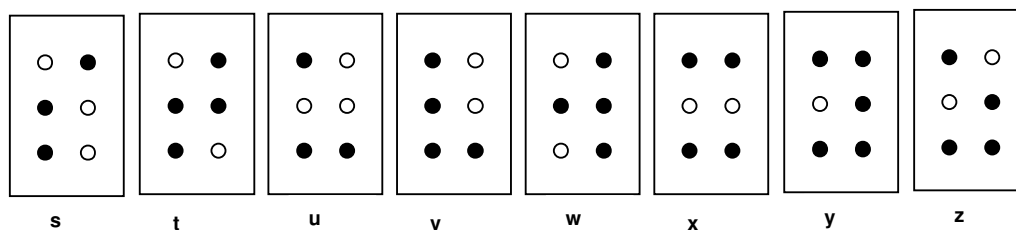
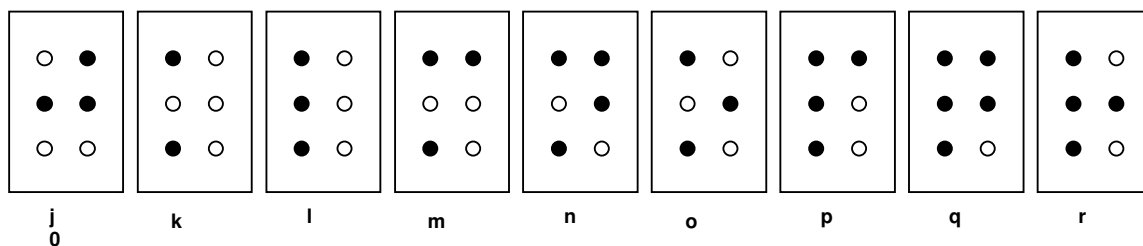
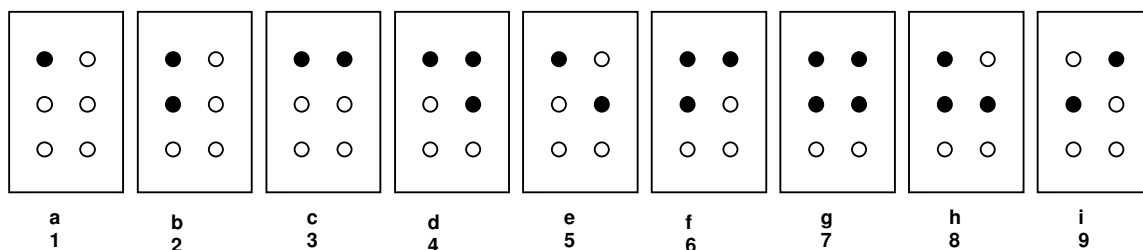
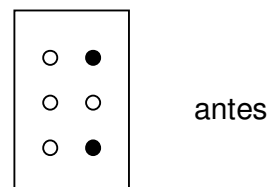
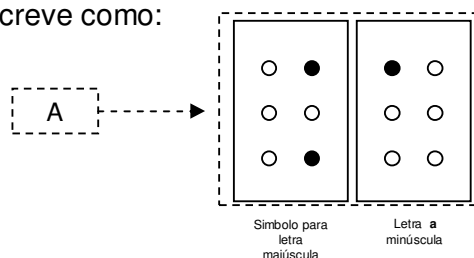
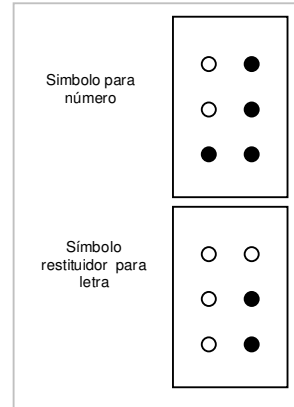
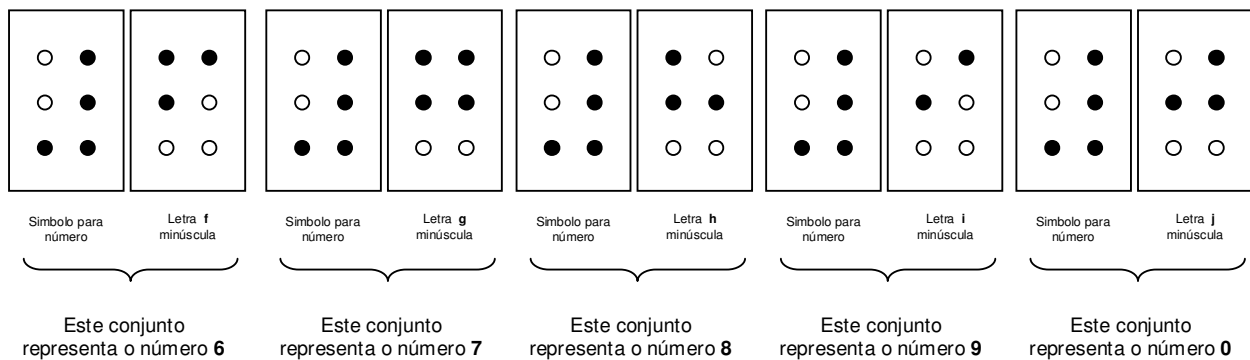
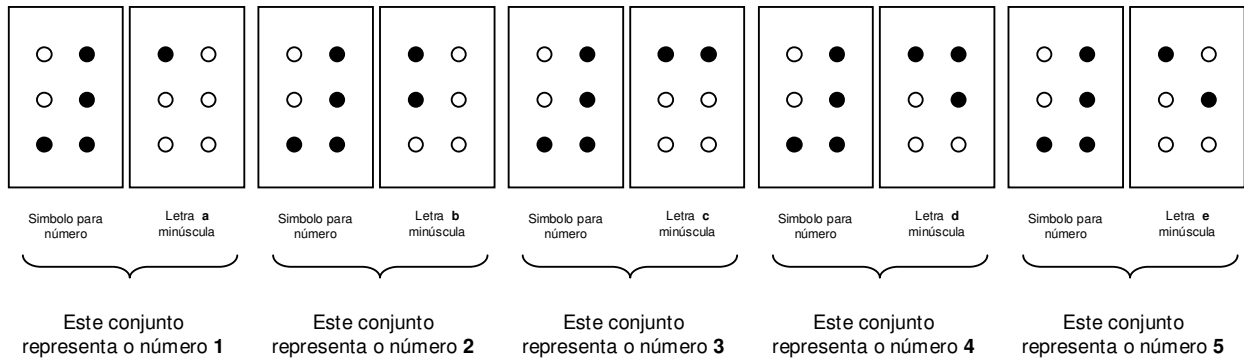
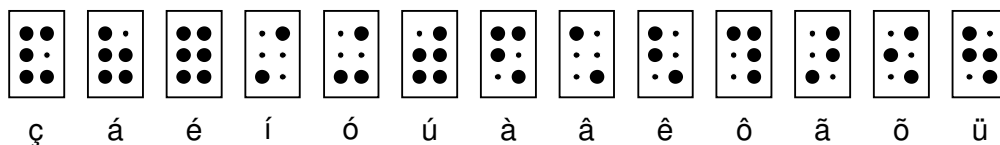
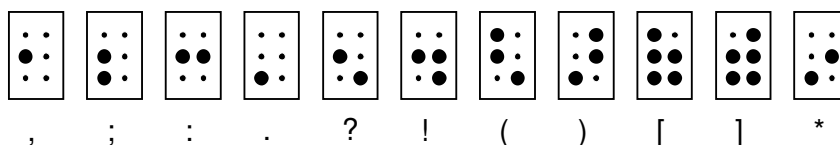
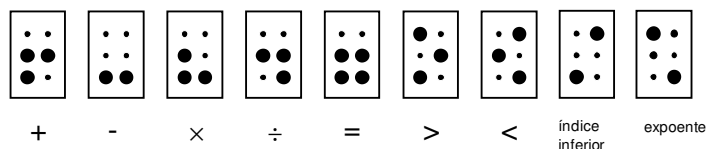
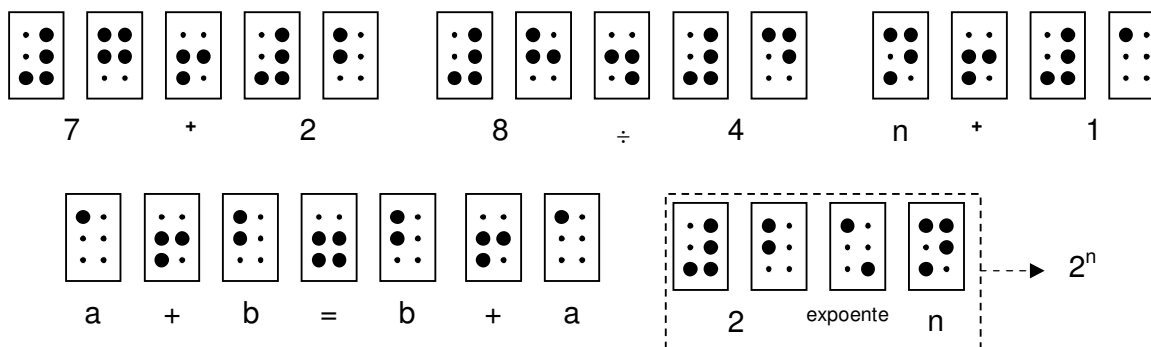
ATIVIDADE: **a)** Quantos diferentes padrões (disposições de pontos) podemos formar usando o sistema 3 x 2 descrito acima?

b) Se quisermos codificar

- todas as letras minúsculas,
- todas as letras maiúsculas,
- os algarismos: 0, 1, 2, 3, 4, 5, 6, 7, 8 e 9,
- os sinais de pontuação: **.** (ponto final), **:** (dois pontos) **?** (ponto de interrogação), **!** (ponto de exclamação) e **,** (vírgula),
- os sinais de operações matemáticas: +, x. – e ÷,

os padrões obtidos nas dimensões 3 x 2 serão suficientes?

c) Quantos padrões podemos formar se dispusermos pontos arranjados em um quadrado 2 x 2? E em um retângulo 1 x 4? Porque será que eles não são usados?

Eis aqui a maneira usual de codificar em Braille as letras minúsculas e os algarismos:

Para codificar letras maiúsculas, usamos o símbolo: antes da letra que desejamos que seja a maiúscula.

Por exemplo, a letra A (maiúscula) se escreve como:

Observe também que a mesma configuração de pontos é usada ora para denotar algumas letras, ora para denotar os algarismos 1, 2, 3, 4, 5, 6, 7, 8, 9 e 0. A fim de evitar confusão, para representar os números, usa-se um símbolo inicial, antecedendo as dez primeiras letras do alfabeto. Quando houver risco de confusão, para voltar novamente a usar o símbolo para significar letras, devemos antecedê-las com outro símbolo inicial, indicando a restauração, ou seja, indicando que os símbolos que virão serão novamente letras.

Vejamos como são as representações dos dez algarismos:

Você deve ter notado na atividade anterior que apenas letras e números não são suficientes para escrever todas as frases que usamos. Na verdade existem muitos outros símbolos que são usados em Braille; eles também variam de país para país. Veja alguns exemplos típicos usados em português:

Todos os sinais gráficos têm representação em Braille. Vejamos alguns:

Vejamos também alguns símbolos usuais da Matemática:

Eis alguns exemplos de expressões matemáticas em Braille:

Para mais informações consulte o site do Instituto Benjamin Constant: http://www.ibc.gov.br/?catid=110&blogid=1&itemid=479.

ATIVIDADES PRÁTICAS COM O CÓDIGO BRAILLE

Esta atividade tem o objetivo de simular a leitura em Braille de frases e fórmulas matemáticas feitas pelos deficientes visuais. Você deve copiar e recortar as fichas e perfurar os círculos marcados em preto com um furador de papel (um clipe ou um palito também podem ser usados).

Depois de recortadas, monte com as fichas algumas expressões matemáticas para que um amigo consiga ler o que você escreveu, mas sem que ele as olhe!

Com as mãos, seu amigo deve sentir as perfurações de cada ficha e, a partir deste ponto, pode consultar a tabela para descobrir o valor da letra ou número correspondente que está "lendo com suas mãos". Mas observe: ele não pode de modo algum ver diretamente a ficha que está manuseando.

Tabela para consulta: Letras e números em Braille

Nas páginas seguintes estão apresentadas as fichas que devem ser manuseadas, em quantidade suficiente para a montagem de fórmulas matemáticas simples em Braille. Copie-as, recorte-as e perfure-as, mãos à obra!

a 1 | a 1 | a 1 | a 1 | a 1 | k

b 2 | b 2 | b 2 | b 2 | b 2 | l

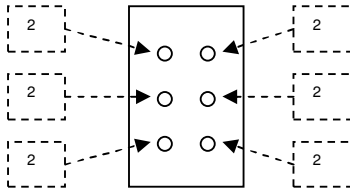
c 3 | c 3 | c 3 | c 3 | c 3 | m

d 4 | d 4 | d 4 | d 4 | d 4 | n

e 5 | e 5 | e 5 | e 5 | e 5 | o >

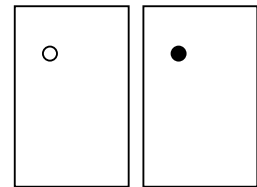
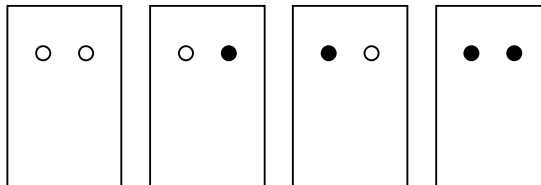
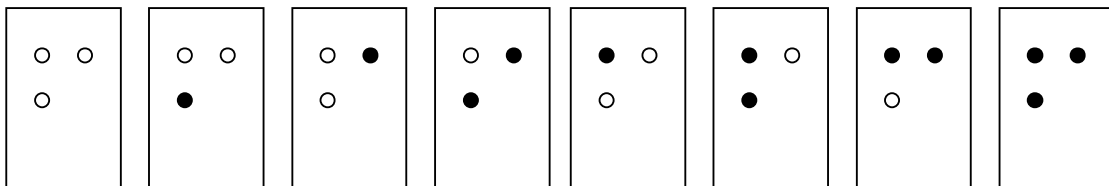
f 6 | f 6 | f 6 | f 6 | f 6 | p

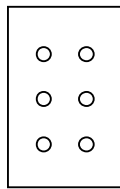
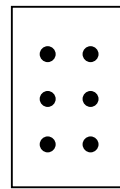
EXPLORANDO CONCEITOS MATEMÁTICOS COM A LINGUAGEM BRAILLE

Existem $2^6 = 64$ configurações que podem ser obtidas no código de Braille usual 3 x 2. É fácil descobrir que isto é verdade, quando aplicamos o Princípio Multiplicativo da Contagem: há duas possibilidades para a primeira casa – ou ela é marcada ou não é (ou pintamos de preto ou de branco) - do mesmo modo há duas possibilidades para cada uma das outras casas, o que resulta em $2 \times 2 \times 2 \times 2 \times 2 \times 2 = 2^6$ possibilidades.

O Princípio Multiplicativo da Contagem:
Se uma decisão puder ser tomada de *m* maneiras diferentes e se, uma vez tomada esta primeira decisão, outra decisão puder ser tomada de *n* maneiras diferentes, então, no total serão tomadas *mxn* decisões.

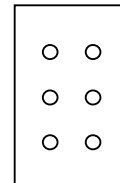
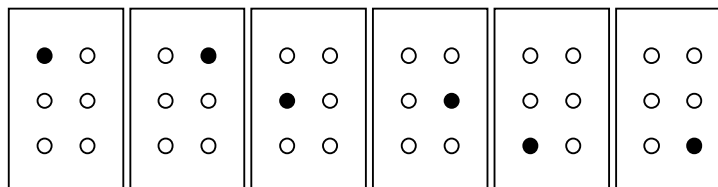
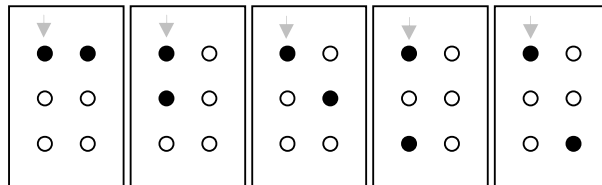
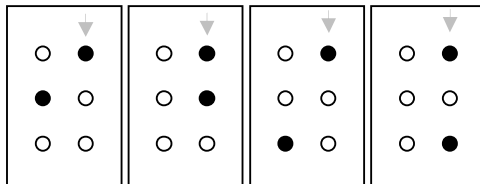
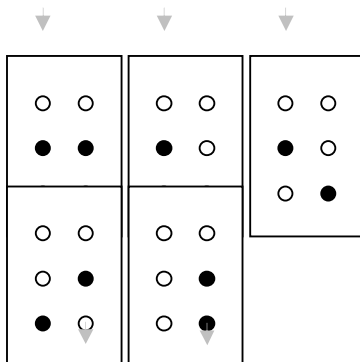
Vale a pena explorar este exemplo com estratégias diferentes.

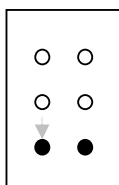
Método 1: Focando na quantidade de pontos - pintados ou não:

Começando com um só ponto, teremos só 2 possibilidades:

Com dois pontos há 4 possibilidades, pois há duas escolhas para cada uma das configurações já vistas acima (com um ponto apenas):

Já com três pontos há 8 possibilidades (duas para cada uma das configurações com dois pontos vistas acima):

Continuando assim, com quatro pontos teremos 16 configurações distintas, com cinco pontos 32 configurações e, é claro, com 6 pontos chegaremos a 64 padrões diferentes de pontos. Isto é fácil de entender: cada configuração em um estágio anterior produz duas novas configurações no estágio seguinte. Dentre as 64 possibilidades, temos dois casos extremos: um

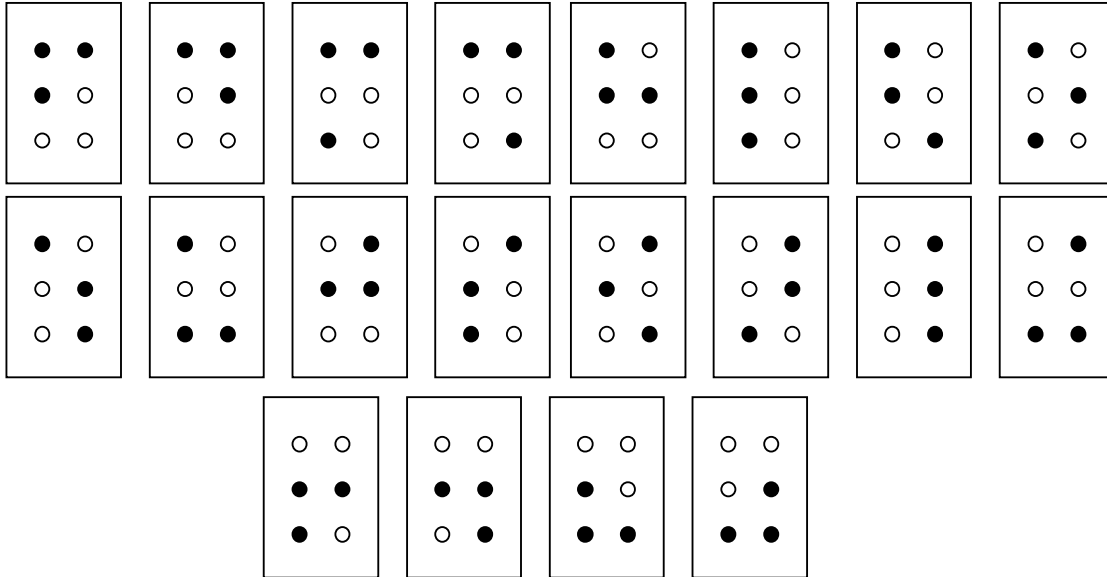
em que nenhum dos pontos é marcado e outro em que todos os seis pontos são marcados:

Em Braille, por motivos óbvios, esta configuração não é usada

Na linguagem Braille, esta configuração tem a função de referencial de posição, para auxiliar a indicar sinais gráficos tais como a crase ou o trema. É usada para indicar a letra acentuada **é**.

Método 2 – Focando na quantidade pintada de pontos

Com nenhum ponto marcado temos apenas uma configuração:

Com apenas um ponto marcado, temos 6 possibilidades:

As configurações com dois pontos marcados totalizam 15. Veja:

Todas estas têm a primeira casa marcada em preto (veja a seta).

Todas estas configurações têm ponto preto na casa com a seta, só está faltando uma que já foi contada, pois ela é a primeira configuração do grupo anterior.

Todas estas têm ponto preto na casa com a seta, mas estão faltando duas que já foram contadas anteriormente.

Todas estas têm ponto preto na casa com a seta, estão faltando três que já foram contadas anteriormente

Resta somente esta última configuração que não apareceu em nenhum dos grupos anteriores.

Deste modo, com dois pontos pretos há 1 + 2 + 3 + 4 + 5 = 15 possibilidades.

Com três pontos marcados em negro, há 20 possibilidades. Veja:

Poderíamos continuar agora exibindo todas as configurações com 4 pontos negros (são 15 ao todo), todas com 5 pontos pretos (são 6 no total) e todas com 6 pontos negros (apenas 1), mas não faremos isto porque há um belo argumento de simetria aqui:

- Escolher 4 pontos para marcar com preto entre 6 pontos brancos é o mesmo que escolher 2 pontos para marcar de branco entre 6 negros!
- De modo análogo, o número de escolhas de 5 pontos para pintá-los de preto dentre 6 pontos brancos é o mesmo número de escolhas de 1 único ponto para pintar de branco dentre 6 pontos negros.
- Simetricamente só há uma possibilidade em que todos os pontos estão marcados e só há uma possibilidade em que todos os pontos não estão marcados.

Resumidamente, temos:

Número de pontos negros	**Número de possíveis configurações**
0	**1**
1	**6**
2	**15**
3	**20**
4	**15**
5	**6**
6	**1**
total	**64**

SIMETRIA

Estes padrões são encontrados nas combinações, que passaremos a estudar.

COMBINAÇÕES MATEMÁTICAS

Existem situações envolvendo contagens em que a ordem dos elementos é importante e outras em que não. Para entender melhor este fato, vamos comparar os dois exemplos abaixo:

1. De quantas maneiras diferentes podemos estacionar 3 carros em 2 garagens?

A resposta é muito simples, se pensarmos da seguinte maneira: existem 3 possibilidades para preencher a primeira garagem, mas apenas duas para a estacionarmos na segunda; pelo Princípio Multiplicativo, o número total de maneira é 3 x 2 = 6 possibilidades. Se A, B e C são os carros, essas 6 maneiras são as seguintes: AB, BA, AC, CA, BC e CB.

2. Quantas saladas de frutas diferentes podemos fazer usando duas das seguintes frutas: abacaxi, banana ou caqui?

Procedemos como antes: primeiro escolhemos umas das três frutas (3 possibilidades), depois a segunda e última fruta (2 possibilidades). Com isto teremos 3 x 2 = 6 possibilidades. Entretanto o número de saladas de frutas não é 6 e sim 3. Porque? Se a, b e c são as frutas, essas 6 escolhas são as seguintes: ab, ba, ac, ca, bc e cb; mas uma salada de frutas feita com abacaxi e banana é a mesma que uma feita com banana e abacaxi, ou seja ab = ba e de modo semelhante, ac = ca e bc = cb. O que é importante observar aqui é que quando duas frutas são permutadas, elas produzem a mesma salada. Neste caso a ordem de escolha das frutas não é importante e o número correto de saladas é

$$\frac{3 \times 2}{2} = 3$$

O número 2 no denominador corresponde à permutação de duas frutas. Ou seja, contamos tudo como se a ordem fosse importante e dividimos o resultado pelo número de permutações de 2 elementos.

Este último exemplo é o protótipo do que se chama em Matemática de uma **combinação simples**. Observe bem o que fizemos:

- Aplicamos o Princípio Multiplicativo para se obter todas as possibilidades, respeitando a ordem (3 x 2 = 6).
- Dividimos o resultado obtido acima pelo número de permutações da quantidade previamente combinada que dá o tamanho de cada escolha (como combinamos fazer saladas com apenas 2 frutas, dividimos por 2! = 2, obtendo (3 x 2)/2 = 3).

No caso geral, se tivermos n objetos distintos à nossa disposição e tivermos que escolher p objetos distintos dentre esses, obteremos as

combinações simples de n elementos tomados p a p. É claro que p deve ser menor ou igual a n.

O número total dessa combinações é denotado por C_n^p e é calculado da seguinte maneira:

$$C_n^p = \frac{n.(n-1)...(n-(p-1))}{p.(p-1).(p-2)...3.2.1}$$, ou, em notação fatorial: $$C_n^p = \frac{n!}{p!(n-p)!}$$

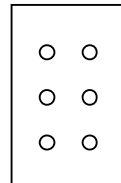
(você sabe justificar porque vale esta última fórmula?).

No exemplo das saladas de frutas, n = 3, p = 2 e o número de saladas de frutas é $C_3^2 = \frac{3!}{2!(3-2)!} = \frac{3.2!}{2!1!} = 3$. Vejamos mais um exemplo:

3. Quantos são os subconjuntos de {a, b, c, d, e} que possuem exatamente três elementos?

A resposta é $C_5^3 = \frac{5!}{3!(5-3)!} = \frac{5.4.3!}{3!2!} = 10$ pois a ordem dos elementos listados em um conjunto não é relevante. De fato os subconjuntos são os seguintes: {a,b,c}, {a,b,d}, {a,b,e}, {a,c,d}, {a,c,e}, {a,d,e}, {b,c,d}, {b,c,e}, {b,d,e}, {c,d,e}.

AS COMBINAÇÕES E A LINGUAGEM BRAILLE

Podemos analisar agora todas as possibilidades da escrita Braille em uma célula 3 x 2:

Neste caso, o número de pontos que podemos combinar entre si é $n = 6$.

Número de pontos em preto	Quantidade de cominações distintas
$p = 0$	$C_6^0 = \frac{6!}{0!(6-0)!} = 1$
$p = 1$	$C_6^1 = \frac{6!}{1!(6-1)!} = 6$
$p = 2$	$C_6^2 = \frac{6!}{2!(6-2)!} = 15$
$p = 3$	$C_6^3 = \frac{6!}{3!(6-3)!} = 20$
$p = 4$	$C_6^4 = \frac{6!}{4!(6-4)!} = 15$
$p = 5$	$C_6^5 = \frac{6!}{5!(6-1)!} = 6$
$p = 6$	$C_6^6 = \frac{6!}{6!(6-6)!} = 1$

Podemos, a partir deste exemplo, inferir algumas conclusões:

- A simetria dos resultados acima sugere que $C_n^p = C_n^{n-p}$. De fato,

$$C_n^p = \frac{n!}{p!(n-p)!} = \frac{n!}{(n-p)!(n-(n-p))!} = C_n^{n-p}$$

- C_n^2 é igual à soma dos n-1 primeiros números naturais. De fato,

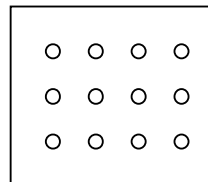
$$C_n^2 = \frac{n!}{2!(n-2)!} = \frac{n.(n-1)}{2} = 1+2+...+(n-1)$$

- $C_n^0 + C_n^1 + C_n^2 + ... + C_n^n = 2^n$

Para ver porque isto é válido, observe que C_n^p é o número de subconjuntos com exatamente p elementos do conjunto {1,2,...,n} e portanto $C_n^0 + C_n^1 + C_n^2 + ... + C_n^n$ é o número total de subconjuntos de {1,2,...,n}. Devemos responder então a seguinte pergunta: quantos são os subconjuntos de {1,2,...,n}?

Para determinar um desses subconjuntos, olhamos para o número 1 e perguntamos: ele está ou não no subconjunto? Existem apenas duas respostas: sim ou não. Olhamos para o número 2 e repetimos a pergunta: 2 está ou não no subconjunto em consideração? Mais uma vez temos duas respostas e continuamos assim até o número n. No total teremos que tomar n decisões e, cada uma delas, admite apenas duas possibilidades. Pelo Princípio Multiplicativo, existirão então 2 x 2 x ... x 2 = 2^n decisões, e como cada decisão determina um e um só subconjunto, teremos que o número total de subconjuntos de {1,2,...,n} é 2^n.

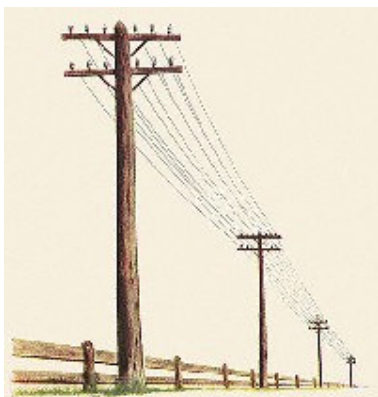
Atividade:

a) Procedendo como na linguagem Braille, se ao invés de uma célula 3 x 2, tivermos uma 3 x 4, como a da figura, quantas configurações diferentes teremos no total?

b) Em uma célula 3 x 4, quantas são as configurações que possuem exatamente 5 pontos marcados?

c) Em uma célula n x m, quantas configurações diferentes podemos formar?

d) Em uma célula n x m, quantas configurações têm exatamente p pontos marcados?

1840

O Código Morse

Samuel Morse (1791-1872), um norte-americano, desenvolveu o código que recebeu o seu nome a fim de enviar mensagens por telégrafo. Trata-se de um alfabeto cifrado em tons curtos e longos. A invenção do telégrafo alterou profundamente a criptografia e tornou imprescindível a cifragem de mensagens.

A	.-	M	--	Y	-.--	6	-....
B	-...	N	-.	Z	--..	7	--...
C	-.-.	O	---	Ä	.-.-	8	---..
D	-..	P	.--.	Ö	---.	9	----.
E	.	Q	--.-	Ü	..--	.	.-.-.-
F	..-.	R	.-.	Ch	----	,	--..--
G	--.	S	...	0	-----	?	..--..
H	....	T	-	1	.----	!	..--.
I	..	U	..-	2	..---	:	---...
J	.---	V	...-	3	...--	“	.-..-.
K	-.-	W	.--	4	....-	‘	.----.
L	.-..	X	-..-	5	.....	=	-...-

O sistema de envio de mensagens a longa distância usado por Morse utilizava o telégrafo (figura); seu suporte físico usava correntes elétricas para controlar eletroímans que funcionavam para emissão ou recepção de sinais. As mensagens eram enviadas usando pulsos (ou tons) elétricos curtos (ponto (.)) e longos (traço (-)) através de linhas telegráficas.

Em 1851, uma conferência internacional em Berlim, estabeleceu uma versão internacional que ainda está em uso até hoje. A mensagem de pedido de socorro SOS, por exemplo, é bem conhecida e tem o seguinte aspecto:

. . . - - - . . .

S   O   S

Vamos entender como o tempo é importante no envio de mensagens, estudando o que ocorre com o Código Morse.

ATIVIDADE: O tempo para envio de uma mensagem com o código Morse é dado pela seguinte tabela:

Caractere	*Tempo*
Ponto (dit)	1 unid de tempo
Traço (dah)	3 unid de tempo
Intervalo entre letras	3 unid de tempo
Intervalo entre palavras	7 unid de tempo

Vejamos qual é o tempo total necessário para enviar um "SOS". Demora-se o tempo de envio de cada letra mais três unidades de tempo entre cada letra.

$3 + 3 + 9 + 3 + 3 = 21$ unidades de tempo

S ↑ O ↑ S

Espaço entre letras Espaço entre letras

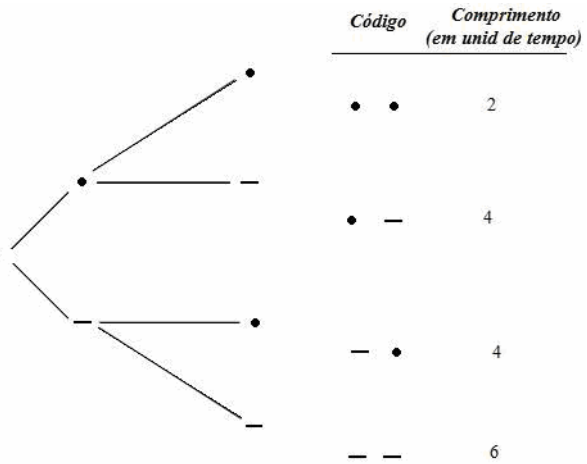
Se pudéssemos usar códigos diferentes para as letras S e O, a fim de que o comprimento da mensagem SOS fosse mais curto, qual seria o menor comprimento possível, utilizando esses novos códigos? Poderíamos usar

Letra	Código	Tempo
S	.	1
O	. .	2
S	.	1

Assim um SOS teria comprimento total igual a 1 + 2 + 1 + 3 + 3 = 10 unidades de tempo (incluindo os espaços entre as letras). Por que os menores códigos não estão associados ao S e ao O? O Código Morse foi projetado para minimizar o tempo de transmissão de qualquer mensagem (em inglês), e não

especificamente para o SOS, ou seja, os códigos de tamanhos mais curtos foram reservados para as letras que ocorrem com mais frequência nesta língua. Na verdade, Morse ao criar o sistema usou a contagem de frequência de letras, às letras mais frequentes foram dados os códigos com menores tempos de transmissão.

Para as letras do alfabeto, usa-se no máximo quatro pontos ou traços e os códigos podem ser constituídos somente por pontos, só por traços ou combinações de ambos.

Uma maneira de encontrar todos os códigos possíveis é usar um diagrama de árvore. Começando por um ponto (comprimento 1), ou um traço (comprimento 3), o próximo conjunto de códigos possui dois pontos ou traços, como mostrado ao lado.

ATIVIDADE: Questão 1: Observe o tempo de transmissão para códigos com 1, 2 ou 3 símbolos:

Código	Tamanho
.	1
–	3

Código	Tamanho
. .	2
. –	4
– .	4
– –	6

Código	Tamanho
. . .	3
. . –	5
. – .	5
– . .	5
– – .	7
– . –	7
. – –	7
– – –	9

Complete o diagrama de árvore até o quarto galho e, para cada letra de código, calcule o tempo de transmissão de cada código obtido.

Questão 2: Compare o tempo de transmissão com a frequência das letras em inglês. A frequência das letras em inglês obedece a ordem: *E T A O N R I S H D L F C U M G P Y W B V K X J Q Z.*

Curiosamente os códigos **não** utilizados por Morse são

Código	Tamanho
..−−	8
.−.−	8
−−−.	10
−−−−	12

Os dois últimos correspondem aos códigos com maior comprimento, mas surpreendentemente os dois primeiros não.

Apesar de sua idade, o Código Morse ainda é utilizado nos dias de hoje e sempre será um meio viável de comunicação de alta confiabilidade em condições difíceis, especialmente quando outros meios falham. Ele sobrevive há mais de 150 anos e a sua longevidade deve-se à forma original e eficiente com que foi criada.

1646 – 1716

Gottfried Wilhelm von Leibniz (1646-1716) foi um importante filósofo e matemático alemão. Ele dizia que decifrar um pictograma é parecido com resolver um problema em Ciência. Se um cientista tem apenas alguns poucos fatos acerca de um fenômeno que deseja explicar, ele pode conceber dezenas de boas teorias, da mesma maneira que um decifrador de códigos pode tentar muitas decifrações para um texto criptografado curto; entretanto se muitos fatos devem ser explicados, o cientista trabalha como o criptógrafo que tenta decifrar um longo texto criptografado. Uma teoria bem formulada deve explicar centenas de fatos particulares e a confiança em sua validade é análoga à que temos quando um longo criptograma está sendo decifrado, já que muitos símbolos devem ser traduzidos simultaneamente.

Leibniz inventou uma máquina de calcular mecânica, revolucionária para a sua época. Leibniz entendeu como funcionava o sistema binário de numeração e abriu as postas para o desenvolvimento da lógica que possibilitou a invenção dos computadores.

A escala binária é utilizada até hoje e sua padronização, conhecida como código ASCII (American Standard Code for Information Interchange), permitiu que máquinas de diferentes fabricantes trocassem dados entre si.

	0	1	2	3	4	5	6	7	10	11	12	13	14	15	16	17
000	NUL	SOM	EOA	EOM	EOT	WRU	RU	BEL	FEO	HT	LF	VT	FF	CR	SO	SI
020	DC0	DC1	DC2	DC3	DC4	ERR	SYN	LEM	S0	S1	S2	S3	S4	S5	S6	S7
040		!	"	#	$	%	&	'	(	)	*	+	,	-	.	/
060	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
100	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
120	P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	↑	←
140																
160													ACK		ESC	DEL

Caracteres imprimíveis em ASCII:

Binário	Decimal	Hexa	Glifo
0010 0000	32	20	
0010 0001	33	21	!
0010 0010	34	22	"
0010 0011	35	23	#
0010 0100	36	24	$
0010 0101	37	25	%
0010 0110	38	26	&
0010 0111	39	27	'
0010 1000	40	28	(
0010 1001	41	29	)
0010 1010	42	2A	*
0010 1011	43	2B	+
0010 1100	44	2C	,
0010 1101	45	2D	-
0010 1110	46	2E	.
0010 1111	47	2F	/
0011 0000	48	30	0
0011 0001	49	31	1
0011 0010	50	32	2
0011 0011	51	33	3
0011 0100	52	34	4
0011 0101	53	35	5
0011 0110	54	36	6
0011 0111	55	37	7
0011 1000	56	38	8
0011 1001	57	39	9
0011 1010	58	3A	:
0011 1011	59	3B	;
0011 1100	60	3C	<
0011 1101	61	3D	=
0011 1110	62	3E	>
0011 1111	63	3F	?

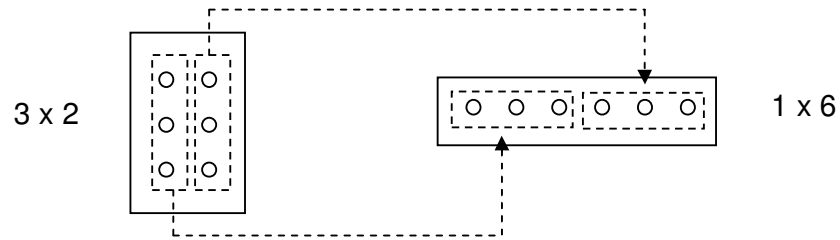
Binário	Decimal	Hexa	Glifo
0100 0000	64	40	@
0100 0001	65	41	A
0100 0010	66	42	B
0100 0011	67	43	C
0100 0100	68	44	D
0100 0101	69	45	E
0100 0110	70	46	F
0100 0111	71	47	G
0100 1000	72	48	H
0100 1001	73	49	I
0100 1010	74	4A	J
0100 1011	75	4B	K
0100 1100	76	4C	L
0100 1101	77	4D	M
0100 1110	78	4E	N
0100 1111	79	4F	O
0101 0000	80	50	P
0101 0001	81	51	Q
0101 0010	82	52	R
0101 0011	83	53	S
0101 0100	84	54	T
0101 0101	85	55	U
0101 0110	86	56	V
0101 0111	87	57	W
0101 1000	88	58	X
0101 1001	89	59	Y
0101 1010	90	5A	Z
0101 1011	91	5B	[
0101 1100	92	5C	\
0101 1101	93	5D	]
0101 1110	94	5E	^
0101 1111	95	5F	_

Binário	Decimal	Hexa	Glifo
0110 0000	96	60	`
0110 0001	97	61	a
0110 0010	98	62	b
0110 0011	99	63	c
0110 0100	100	64	d
0110 0101	101	65	e
0110 0110	102	66	f
0110 0111	103	67	g
0110 1000	104	68	h
0110 1001	105	69	i
0110 1010	106	6A	j
0110 1011	107	6B	k
0110 1100	108	6C	l
0110 1101	109	6D	m
0110 1110	110	6E	n
0110 1111	111	6F	o
0111 0000	112	70	p
0111 0001	113	71	q
0111 0010	114	72	r
0111 0011	115	73	s
0111 0100	116	74	t
0111 0101	117	75	u
0111 0110	118	76	v
0111 0111	119	77	w
0111 1000	120	78	x
0111 1001	121	79	y
0111 1010	122	7A	z
0111 1011	123	7B	{
0111 1100	124	7C	|
0111 1101	125	7D	}
0111 1110	126	7E	~

Para entender como funcionam este e outros códigos similares, vamos rever o sistema numérico usado pelos computadores: o sistema binário de numeração.

O SISTEMA BINÁRIO

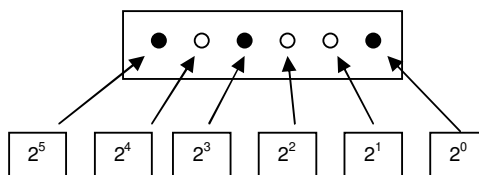
Aproveitando nossa experiência com o sistema Braille, vamos estudar agora um sistema análogo em que as células possuem uma linha e seis colunas. Ele será muito semelhante ao sistema usual da linguagem Braille 3 x 2,

pois existe uma correspondência um-a-um entre as configurações com células 3 x 2 e configurações em células 1 x 6. Veja:

Sistemas do tipo 1 x n servem para escrever números na base 2 e, assim sendo, têm muitas aplicações na Matemática e na Informática, como é o caso do Código ASCII apresentado anteriormente.

Podemos escrever qualquer número natural na base 2, utilizando-se para isto apenas os dígitos 0 e 1. Para compreender como isto pode ser realizado, trabalharemos, por simplicidade, com os números que vão de 0 a 63.

Dado um número qualquer (tomaremos como exemplo o número 41), veja como agrupar para escrever o número na base 2:

Conclusão: $41 = \mathbf{1} \times 2^5 + \mathbf{0} \times 2^4 + \mathbf{1} \times 2^3 + \mathbf{0} \times 2^2 + \mathbf{0} \times 2^1 + \mathbf{1} \times 2^0$. Esta expressão é escrita abreviadamente na seguinte forma: $41 = (\mathbf{1\ 0\ 1\ 0\ 0\ 1})_2$ (lê-se: 41 é um, zero, um, zero, zero, um, na base 2).

Veja como representá-lo no estilo Braille:

Os números de 0 a 63 podem ser representados na base 2, de acordo com o seguinte diagrama de árvore:

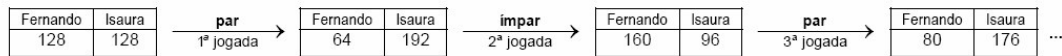
Número	Braille
000000	○ ○ ○ ○ ○ ○
000001	○ ○ ○ ○ ○ ●
000010	○ ○ ○ ○ ● ○
000011	○ ○ ○ ○ ● ●
000100	○ ○ ○ ● ○ ○
000101	○ ○ ○ ● ○ ●
000110	○ ○ ○ ● ● ○
000111	○ ○ ○ ● ● ●
001000	○ ○ ● ○ ○ ○
001001	○ ○ ● ○ ○ ●
001010	○ ○ ● ○ ● ○
001011	○ ○ ● ○ ● ●
001100	○ ○ ● ● ○ ○
001101	○ ○ ● ● ○ ●
001110	○ ○ ● ● ● ○
001111	○ ○ ● ● ● ●
010000	○ ● ○ ○ ○ ○
010001	○ ● ○ ○ ○ ●
010010	○ ● ○ ○ ● ○
010011	○ ● ○ ○ ● ●
010100	○ ● ○ ● ○ ○
010101	○ ● ○ ● ○ ●
010110	○ ● ○ ● ● ○
010111	○ ● ○ ● ● ●
011000	○ ● ● ○ ○ ○
011001	○ ● ● ○ ○ ●
011010	○ ● ● ○ ● ○
011011	○ ● ● ○ ● ●
011100	○ ● ● ● ○ ○
011101	○ ● ● ● ○ ●
011110	○ ● ● ● ● ○
011111	○ ● ● ● ● ●
100000	● ○ ○ ○ ○ ○
100001	● ○ ○ ○ ○ ●
100010	● ○ ○ ○ ● ○
100011	● ○ ○ ○ ● ●
100100	● ○ ○ ● ○ ○
100101	● ○ ○ ● ○ ●
100110	● ○ ○ ● ● ○
100111	● ○ ○ ● ● ●
101000	● ○ ● ○ ○ ○
101001	● ○ ● ○ ○ ●
101010	● ○ ● ○ ● ○
101011	● ○ ● ○ ● ●
101100	● ○ ● ● ○ ○
101101	● ○ ● ● ○ ●
101110	● ○ ● ● ● ○
101111	● ○ ● ● ● ●
110000	● ● ○ ○ ○ ○
110001	● ● ○ ○ ○ ●
110010	● ● ○ ○ ● ○
110011	● ● ○ ○ ● ●
110100	● ● ○ ● ○ ○
110101	● ● ○ ● ○ ●
110110	● ● ○ ● ● ○
110111	● ● ○ ● ● ●
111000	● ● ● ○ ○ ○
111001	● ● ● ○ ○ ●
111010	● ● ● ○ ● ○
111011	● ● ● ○ ● ●
111100	● ● ● ● ○ ○
111101	● ● ● ● ○ ●
111110	● ● ● ● ● ○
111111	● ● ● ● ● ●

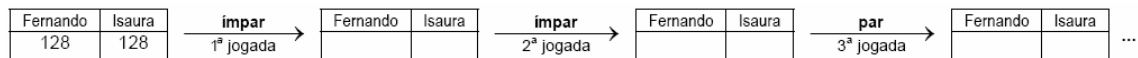
ATIVIDADE: Resolva o seguinte problema, estabelecendo relações com o sistema binário:

(4) Fernando e Isaura inventaram um jogo diferente, cujas regras são as seguintes:

1. eles começam uma partida com 128 palitos cada um;
2. em cada jogada, eles tiram par ou ímpar; se sai par, Fernando dá metade dos palitos que tem para Isaura e, se sai ímpar, Isaura dá a metade dos palitos que tem para Fernando.
3. eles repetem o procedimento da regra 2 até que um deles fique com um número ímpar de palitos, quando a partida acaba. Ganha quem ficar com maior número de palitos.

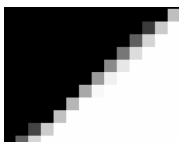
Veja o que acontece em uma partida onde a seqüência das três primeiras jogadas é **par**, **ímpar**, **par**:

Fernando	Isaura		Fernando	Isaura		Fernando	Isaura		Fernando	Isaura	
128	128	**par** → 1ª jogada	64	192	**impar** → 2ª jogada	160	96	**par** → 3ª jogada	80	176	...

(a) Complete o esquema com o número de palitos de Fernando e Isaura, de acordo com as jogadas indicadas.

Fernando	Isaura		Fernando	Isaura		Fernando	Isaura		Fernando	Isaura	
128	128	**impar** → 1ª jogada			**impar** → 2ª jogada			**par** → 3ª jogada			...

(b) Uma partida acabou quando Fernando ficou com 101 palitos. Na última jogada saiu par ou ímpar?

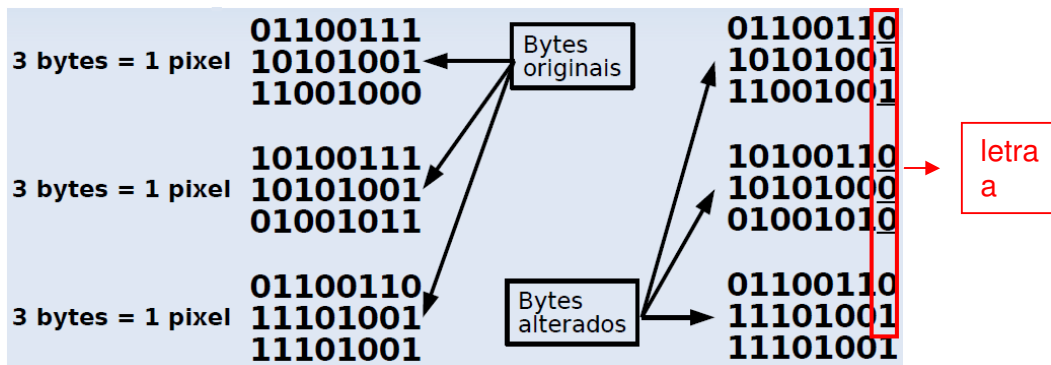
(c) Qual foi a seqüência de pares e ímpares da partida que acabou quando Fernando ficou com 101 palitos?

(d) Mostre que qualquer partida acaba com exatamente sete jogadas.

COMO ESCONDER INFORMAÇÃO EM UMA IMAGEM DIGITAL

As imagens digitais são construídas a partir de uma unidade básica chamada pixel. Um **pixel** é o menor elemento em um dispositivo de exibição (como por exemplo um monitor de vídeo), ao qual é possivel atribuir-se uma cor. A cor de cada pixel é determinada por uma sequência definida de zeros e uns, ou seja, por um número binário (em geral um número grande dividido em grupos menores de mesmo tamanho chamados bytes - um **byte** é um conjunto de bits adjacentes que carrega uma informação, por exemplo um caractere). Números próximos geram cores próximas. Se dois números estiverem muito próximos, as cores a eles associadas podem ser imperceptíveis ao olho humano e esta nossa "incapacidade" visual pode ser explorada para embutir em uma imagem inocente uma mensagem secreta.

Como fazer isto? Existem muitos métodos, mas o mais simples deles pode ser executado através da alteração do dígito menos significativo, pois esta alteração é a que torna o número original e o modificado os mais próximos possíveis e, portanto, as cores a eles associados serão também bastante próximas. Vamos entender isto melhor; por exemplo, se quisermos modificar algum dígito do número 347187, qual deve ser o dígito que devemos alterar para obter um número próximo? Certamente o dígito 7 da casa das unidades.

Vamos esconder, para exemplificar, a letra "a" em uma imagem, podendo da seguinte maneira:

- escrevemos a letra "a" em alguma forma binária: usando o código ASCII a letra pode ser coficidada por 01100001,
- escolhemos uma imagem, descrita por seus bytes que compõem seus píxeis,
- alteramos o último algarismo desses bytes se eles não forem os mesmos da letra "a" e os mantemos se forem iguais.

Observe que nem todos os bytes foram alterados; as imagens associadas aos bytes originais e aos modificados serão muito próximas e no entanto a letra "a" ficou embutida na imagem.

UM PEQUENO COMPUTADOR DE PAPEL – OS CARTÕES BINÁRIOS

Vamos utilizar cartões de cartolina perfurados para trabalhar com números de 0 a 31, utilizando-se a base 2. Esses números podem ser escritos com apenas 5 dígitos, observe:

Base 10	Base 2	Base 10	Base 2	Base 10	Base 2	Base 10	Base 2
0	00000	8	01000	16	10000	24	11000
1	00001	9	01001	17	10001	25	11001
2	00010	10	01010	18	10010	26	11010
3	00011	11	01011	19	10011	27	11011
4	00100	12	01100	20	10100	28	11100
5	00101	13	01101	21	10101	29	11101
6	00110	14	01110	22	10110	30	11110
7	00111	15	01111	23	10111	31	11111

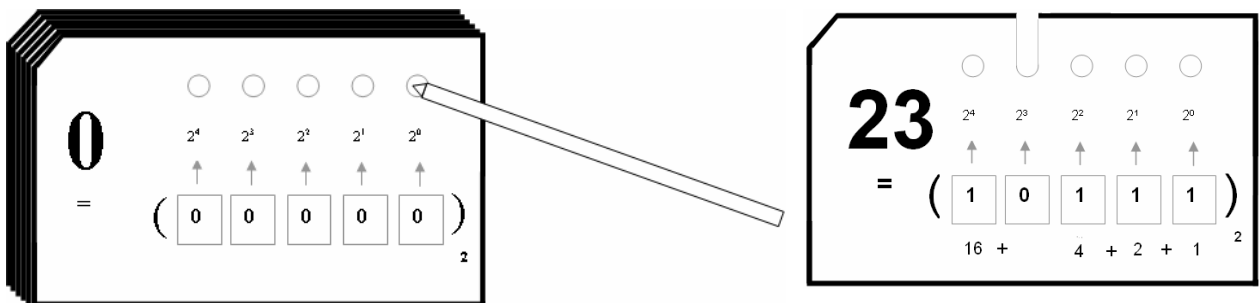
a) Copie, recorte, perfure e corte as fendas dos cartões das páginas seguintes.

b) Cada buraco representará o número 1 e cada fenda o número 0. Faça um maço com as cartas. Se você colocar um palito (ou um canudo ou um clipe) por alguns dos buracos do maço, e levantá-lo, algumas cartas cairão e outras ficarão presas no palito. Repetindo organizadamente este procedimento você poderá realizar várias operações com os números binários de 0 a 31. Veja algumas delas:

- Separar as cartas pares da ímpares. Basta colocar o palito no primeiro furo à direita e levantar. Todas os cartões com números pares cairão.
- Com somente 5 colocações do palito e levantamentos é possível colocar as cartas de 0 a 31 em ordem crescente. Embaralhe as cartas. Comece colocando o palito no primeiro buraco da direita (casa das unidades). Com cuidado levante o maço, deixando que as cartas caiam, mas mantendo a ordem. Coloque as cartas que caíram na frente das demais

e repita o mesmo procedimento para todos os demais 4 buracos, sempre mantendo a ordem. Quanto terminar as cartas estarão em ordem.

- Pode-se localizar qualquer número de 0 a 31 com a colocação do palito e levantamento do maço 5 vezes. Isto se deve ao fato de que qualquer número natural tem representação única na base 2. Veja como você pode fazer para localizar a carta 23:

Coloque o palito na casa das unidades e levante o maço, descarte as que caíram. A seguir coloque no buraco 2^1, levante e descarte as que caíram. Prossiga, colocando o palito na casa 2^2, descarte as que caíram. Coloque na casa 2^3, levante e descarte as que ficaram presas. Agrupe as cartas que caíram nesta última vez e finalmente use o palito na casa 2^4. A carta que ficou presa é a 23.

ATIVIDADE:

1. Se fizermos cartas com 6 buracos ao invés de 5, quantos números diferentes obteremos?

2. Qual é o número mínimo de buracos que teremos fazer nos cartões para representar os números de 0 até 127?

3. Leia a próxima atividade “O dia do aniversário” e descreva uma maneira de adivinhar o aniversário de uma pessoa usando os cartões perfurados que você fabricou.

31
2^4 2^3 2^2 2^1 2^0
= (1 1 1 1 1) 2
16 + 8 + 4 + 2 + 1
30
2^4 2^3 2^2 2^1 2^0
= (1 1 1 1 0) 2
16 + 8 + 4 + 2
29
2^4 2^3 2^2 2^1 2^0
= (1 1 1 0 1) 2
16 + 8 + 4 + 1
28
2^4 2^3 2^2 2^1 2^0
= (1 1 1 0 0) 2
16 + 8 + 4
27
2^4 2^3 2^2 2^1 2^0
= (1 1 0 1 1) 2
16 + 8 + 2 + 1
26
2^4 2^3 2^2 2^1 2^0
= (1 1 0 1 0) 2
16 + 8 + 2
25
2^4 2^3 2^2 2^1 2^0
= (1 1 0 0 1) 2
16 + 8 + 1
24
2^4 2^3 2^2 2^1 2^0
= (1 1 0 0 0) 2
16 + 8
23
2^4 2^3 2^2 2^1 2^0
= (1 0 1 1 1) 2
16 + 4 + 2 + 1
22
2^4 2^3 2^2 2^1 2^0
= (1 0 1 1 0) 2
16 + 4 + 2

21
2^4 2^3 2^2 2^1 2^0
= (1 0 1 0 1)2
16 + 4 + 1
20
2^4 2^3 2^2 2^1 2^0
= (1 0 1 0 0)2
16 + 4
19
2^4 2^3 2^2 2^1 2^0
= (1 0 0 1 1)2
16 + 2 + 1
18
2^4 2^3 2^2 2^1 2^0
= (1 0 0 1 0)2
16 + 2
17
2^4 2^3 2^2 2^1 2^0
= (1 0 0 0 1)2
16 + 1
16
2^4 2^3 2^2 2^1 2^0
= (1 0 0 0 0)2
16
15
2^4 2^3 2^2 2^1 2^0
= (0 1 1 1 1)2
8 + 4 + 2 + 1
14
2^4 2^3 2^2 2^1 2^0
= (0 1 1 1 0)2
8 + 4 + 2
13
2^4 2^3 2^2 2^1 2^0
= (0 1 1 0 1)2
8 + 4 + 1
12
2^4 2^3 2^2 2^1 2^0
= (0 1 1 0 0)2
8 + 4

11
2^4 2^3 2^2 2^1 2^0
= (0 1 0 1 1)$_2$
8 + 2 + 1
10
2^4 2^3 2^2 2^1 2^0
= (0 1 0 1 0)$_2$
8 + 2
9
2^4 2^3 2^2 2^1 2^0
= (0 1 0 0 1)$_2$
8 + 1
8
2^4 2^3 2^2 2^1 2^0
= (0 1 0 0 0)$_2$
8
7
2^4 2^3 2^2 2^1 2^0
= (0 0 1 1 1)$_2$
4 + 2 + 1
6
2^4 2^3 2^2 2^1 2^0
= (0 0 1 1 0)$_2$
4 + 2
5
2^4 2^3 2^2 2^1 2^0
= (0 0 1 0 1)$_2$
4 + 1
4
2^4 2^3 2^2 2^1 2^0
= (0 0 1 0 0)$_2$
4
3
2^4 2^3 2^2 2^1 2^0
= (0 0 0 1 1)$_2$
2 + 1
2
2^4 2^3 2^2 2^1 2^0
= (0 0 0 1 0)$_2$
2

1 = (0 0 0 0 1)2
1
0 = (0 0 0 0 0)2
2^4 2^3 2^2 2^1 2^0
CARTÕES RESERVA

Atividade : O dia do aniversário e o sistema binário

MÁGICA MATEMÁTICA

Para adivinhar o dia que uma pessoa nasceu

Um sim um não

dom	seg	ter	qua	qui	sex	sab
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

De dois em dois

dom	seg	ter	qua	qui	sex	sab
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

De quatro em quatro

dom	seg	ter	qua	qui	sex	sab
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

De oito em oito

dom	seg	ter	qua	qui	sex	sab
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

Meio mês sim meio não

dom	seg	ter	qua	qui	sex	sab
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

COMO FUNCIONA O TRUQUE

Como adivinhar o dia em que uma pessoa nasceu:

1. Peça à pessoa que indique em quais dos calendários a data de seu nascimento aparece sublinhada.
2. Some os **primeiros** números sublinhados que aparecem nos calendários que a pessoa escolheu e você descobrirá a data de seu aniversário, sem que ela lhe conte.

Exemplo: Se a pessoa nasceu no dia 7, os calendários em que este número aparece sublinhado são: o primeiro, o segundo e o terceiro. Somando os **primeiros números sublinhados** destes três calendários teremos **1 + 2 + 4 = 7**. Não é legal? Se você seguir o roteiro abaixo, poderá descobrir o signo e também o mês que a pessoa nasceu .

Como adivinhar o mês em que uma pessoa nasceu – consulte seu horóscopo para encontrar o mês de nascimento:

Áries 21 de março a 20 de abril
Hoje é um dia muito favorável para lidar com cálculos matemáticos. Abra sua mente para a beleza da Matemática e não deixe de acreditar no seu potencial criativo. Você nasceu no dia ...

Touro 21 de abril a 20 de maio
Um ciclo de novas idéias se abre para você. Tudo se alterna tal qual uma função trigonométrica. É tempo de estudar e desenvolver os seus potenciais criativos. Você nasceu no dia...

Gêmeos 21 de maio a 20 de junho
Hoje é um dia em que muitas coisas não caminham muito de acordo com seus planos, mas lembre-se que problemas devem estar nos livros de Matemática e mesmo assim eles podem ser solucionados! Você nasceu no dia ...

Câncer 21 de junho a 21 de julho
Alegre-se! Hoje é um dia harmonioso para você interagir, fazer novas amizades e dar início a projetos pessoais como o estudo da Matemática. Você nasceu no dia ...

Leão 22 de julho a 22 de agosto
Problemas existem, mas com disposição, talento e criatividade você vence qualquer obstáculo. Quando estudar Matemática, não desista, a solução sempre estará a seu alcance. Você nasceu no dia ...

Virgem 23 de agosto a 22 de setembro
Hoje é um dia de muita sensibilidade e pensamento positivo. Realize hoje mesmo seus sonhos, estudando Matemática com dedicação. Acredite no seu potencial. Você nasceu no dia ...

Libra 23 de setembro a 22 de outubro
Hoje é um dia favorável para lidar com os assuntos da Geometria. Comece investindo no seu visual e surpreenda a todos, principalmente seu professor, fazendo todos os exercícios de Matemática. Você nasceu no dia ...

Escorpião 23 de outubro a 21 de novembro
É bem provável que o que você esteja procurando externamente esteja dentro de você, por isto, resolva você mesmo seus problemas de Matemática, sem procurar ajuda. Você consegue! Você nasceu no dia ...

Sagitário 22 de novembro a 21 de dezembro
Descubra seu potencial criativo, resolvendo problemas de Matemática. Com isso estará afastando a rotina e admirando a beleza desta ciência. Observe o mundo com os olhos da razão! Você nasceu no dia ...

Capricórnio 22 de dezembro a 20 de janeiro
Não se aborreça com pequenos atritos do dia-a-dia. Não de deixe abalar quando não encontrar imediatamente a solução de um problema de Matemática. Não desista e entenda que há propósitos maiores cujas portas serão abertas pela dedicação e estudo. Você nasceu no dia ...

Aquário 21 de janeiro a 19 de fevereiro
Hoje a vida lhe dará tudo para ser feliz. Há tesouros que temos e muitas vezes não os percebemos; por exemplo, há uma satisfação enorme quando resolvemos um belo problema de Matemática. Você nasceu no dia ...

Peixes 20 de fevereiro a 20 de março
Hoje é um dia de oportunidades e novidades, principalmente nos estudos. Você irá resolver com facilidade todos os problemas de Matemática que lhe forem apresentados. É tempo fazer planos, trabalhar as idéias criativas e executá-las. Você nasceu no dia...

Podemos implementar todas as operações que são realizadas na base 10 também na base 2. Existem máquinas simples que ajudam a entender como estas operações são feitas.

As fotos ao lado mostram uma máquina que efetua adições no sistema binário com bolinhas de gude. Para ver o funcionamento da máquina consulte o site: http://www.youtube.com/watch?v=GcDshWmhF4A&NR=1 Para ver detalhes de sua construção acesse: http://www.youtube.com/watch?v=md0TISjIags&feature=related

Continuamos agora nossa viagem histórica pelo reino da Criptologia.

Século XX

AS GRANDES GUERRAS MUNDIAIS

Você já pensou nisto?

A Primeira Guerra Mundial foi à guerra dos químicos – gás mostarda e o cloro.

A Segunda Guerra Mundial foi à guerra dos físicos – bomba atômica.

A Terceira Guerra Mundial seria a guerra dos matemáticos? – controle sobre a informação.

Criptografia eletro-mecânica

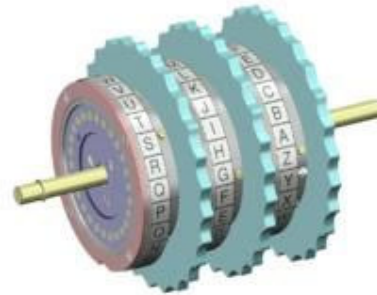
Durante a Primeira e Segunda Guerras Mundiais proliferaram artefatos mecânicos construídos especialmente para o envio de mensagens secretas. A máquina Enigma foi um equipamento especialmente projetado para cifrar mensagens, constituindo-se um dos segredos mais bem guardados na

Segunda Grande Guerra. Ela era usada pelos alemães para proteger as comunicações entre o comando e as embarcações navais.

ATIVIDADES COM A MÁQUINA ENIGMA

Como a máquina Enigma funciona

Quando uma letra do texto é pressionada no teclado, uma corrente elétrica passa pelos diversos componentes de cifragem da máquina, acendendo uma luz no "painel de lâmpadas", a letra acendida é a codificação da letra digitada. O que faz a máquina Enigma tão especial é o fato de que cada vez que uma letra é pressionada, as peças móveis da máquina mudam de posição e, se numa próxima vez que a mesma letra for teclada, provavelmente será cifrada como algo diferente. Isto implica imunidade aos métodos tradicionais de análise de frequência de letras, ou seja, a máquina não se enquadra no estilo Júlio César.

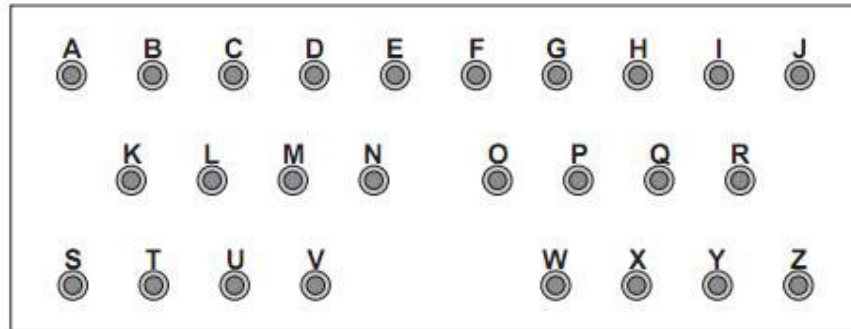
Para tornar ainda mais difícil, diferentes partes da máquina podem ser configuradas de diferentes maneiras. A menos que se saiba a configuração inicial da máquina, não se pode, em um tempo curto, decifrar as mensagens geradas por ela. Dentro da máquina Enigma há três discos com cifras; estes discos são chamados de rotores e eles podem ser retirados e trocados. Cada rotor tem as letras de A a Z, com diferentes sistemas internos de fiação. A marinha alemã dispunha de cinco rotores que o operador poderia escolher para serem colocados no espaço interno da máquina, previsto para três.

ATIVIDADE: a) De quantas maneiras diferentes podemos posicionar cinco rotores nas três diferentes posições da máquina Enigma?

b) Cada rotor pode ser posicionado inicialmente em 26 posições, uma para cada letra do alfabeto. Com três rotores, quantas são as possibilidades de posicionamento inicial?

Os rotores são conectados entre si. Cada vez que uma letra é digitada, o rotor do canto direito gira em uma posição. O rotor do meio gira uma posição após o primeiro rotor passar pelas 26 letras. Da mesma forma, o rotor da esquerda anda uma posição após o rotor do meio passar pelas suas 26 posições; o sistema é aproximadamente similar ao mecanismo de contagem de quilômetros de um automóvel (hodômetro), exceto que o giro do rotor passa por vinte e seis posições em vez de dez.

Depois de resolver a atividade acima, é fácil concluir que existem

possibilidades para configurar inicialmente os rotores da máquina. Isto dá 1054560 maneiras diferentes. Portanto, existem mais de um milhão de

configurações possíveis para a posição inicial da máquina - mas ela é ainda mais complicada! Além das disposições mecânicas dos rotores, há as conexões elétricas (iguais aos centros telefônicos antigos). Na frente da máquina há uma placa de conexões de cabos elétricos. Ela é usada para embaralhar ainda mais as mensagens e aumentar o número de configurações iniciais.

Usando cabos com plugues nas extremidades, pode-se conectar pares de letras. Se, por exemplo, conectarmos A a B então, ao digitar a letra A, a corrente elétrica segue o caminho associado à letra B, e vice-versa.

Usando-se apenas um cabo, quantas diferentes conexões podemos formar? A resposta é $S_{25} = 25 + 24 + 23 + 22 + ...+ 2 + 1 = (25.26)/2 = 325$ maneiras. Isto porque colocando-se um plug em A, há 25 possibilidades de conexões com as outras letras. Colocando-se em B, há 24 possibilidades pois a conexão AB é a mesma que a BA, colocando-se em C, há 23 outras conexões diferentes e assim sucessivamente até a última conexão YZ.

$$S_{25} = 25 + 24 + \ldots + 2 + 1$$

$$S_{25} = 1 + 2 + \ldots + 24 + 25$$

$$2\,S_{25} = \underbrace{26 + 26 + \ldots + 26 + 26}_{25 \text{ vezes}} = 25 \times 26$$

$$S_{25} = \frac{25 \times 26}{2} \qquad \left(\text{ou } S_n = \frac{n(n+1)}{2}\right)$$

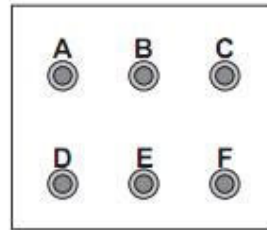
$$= 325 \text{ maneiras}$$

ATIVIDADE: Com a placa de conexões simplificada da figura ao lado, quantas ligações diferentes podemos fazer ao utilizar:

a) um cabo apenas

b) dois cabos

c) três cabos

d) quatro cabos?

A atividade acima mostra o quão complicado pode ser, mesmo com apenas 6 letras, encontrar o número total de conexões. Na verdade, a fórmula para o número de maneiras de escolher m pares (não ordenados) dentre n objetos é

$$\frac{n!}{(n-2m)!\,m!\,2^m}$$

De fato, começamos primeiro a selecionar 2m dos n itens, respeitando a ordem. Ao escolher o primeiro item, temos n opções. Ao escolher o segundo item, temos n – 1 opções ...ao escolher o 2m-ésimo item, temos (n – 2m) + 1 opções. Assim, no total temos $n\times(n-1)\times(n-2)\times\ldots\times(n-2m+1)$ escolhas ordenadas. Isto pode ser escrito como

$$\frac{n!}{(n-2m)!}$$

Infelizmente, algumas dessas combinações de m pares de n elementos são as mesmas, já que não nos interessam pares ordenados e nem a localização de um par na escolha feita. Precisamos descontar esta contagem excessiva. Vamos aos descontos: os m pares podem ser escolhidos em qualquer ordem, assim temos m opções para o primeiro par, m – 1 opções para o segundo par e assim por diante até que haja 1 opção para o último par. Isto dá $m\times(m-1)\times\ldots\times2\times1$ maneiras. Portanto, há m! maneiras de organizar os m pares. Além disso, a posição de um elemento dentro de um par não é

importante e o número de descontos deve ser multiplicado por 2 para cada um dos m pares. Isto é o mesmo que descontar por 2^m.

No total teremos então que um conjunto de m pares tem m! × 2^m combinações que podem ser identificadas, já que a ordem não é levada em conta.

Precisamos dividir o número de maneiras de escolher 2m itens por este valor porque só precisamos contar uma vez cada uma das m! × 2^m combinações equivalentes.

Nosso número final de maneiras de escolher m pares dentre n elementos é portanto:

$$\frac{\frac{n!}{(n-2m)!}}{m!\,2^m} = \frac{n!}{(n-2m)!\,m!\,2^m}$$

Exemplo: De quantas maneiras podemos escolher 2 pares dentre 6 objetos?

Solução: Aqui, n = 6 e m = 2, assim o número de maneiras é

$$\frac{6!}{2!\,2!\,4} = 45$$

(e isto é o que você deve ter obtido na atividade anterior, ítem b). Verifique para os outros itens. O que acontece com 4 cabos?).

Exemplo: Quantas maneiras existem de escolher 10 pares de 26 letras?

Solução: n = 26, m = 10, então a partir da fórmula o número de maneiras é

$$\frac{26!}{6!\,10!\,2^{10}} = 150738274937250 \approx 1{,}5 \times 10^{14}$$

Finalmente podemos calcular o número aproximado de configurações dos circuitos elétricos da máquina Enigma de três rotores; o número é

$$60 \times 17576 \times 1,5 \times 10^{14} = 1,58 \times 10^{20}$$

Nº de configurações para os rotores

Nº de configurações da placa de conexões

que é um número muito, muito grande!

O processo de decifração da máquina Enigma

O processo de decifração é extremamente simples, desde que o receptor da mensagem saiba como a máquina Enigma foi configurada quando a mensagem foi cifrada.

Um soldado alemão ao receber uma mensagem cifrada tinha apenas que digitar as letras cifradas em sua própria máquina. Se sua máquina tivesse configurada exatamente da mesma forma como a do remetente da mensagem, as letras que apareceriam no painel de lâmpadas formariam o texto original.

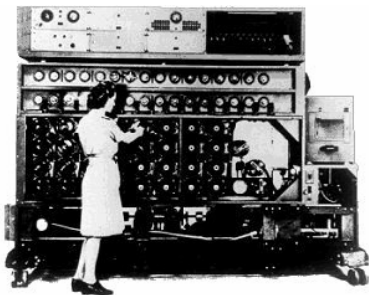
É desta forma que funciona o algoritmo ou método de criptografia da máquina Enigma. A chave é saber como a máquina foi inicialmente configurada.

Como vimos, este tipo de criptografia é conhecido como criptografia simétrica porque a operação de decifrar é inversa à operação de cifrar. A chave de decodificação é também a mesma chave de codificação. Isto significa que se o inimigo souber o seu método de encriptação (e durante a II Guerra Mundial, os aliados sabiam que os alemães estavam usando a Enigma), saberia decifrar as mensagens. A chave deve ser mantida em segredo.

A fim de tornar o mais difícil possível para os aliados descobrirem a chave da Enigma, os alemães alteravam a chave a cada dia, reconfigurando suas máquinas todas as noites, à meia-noite. Os operadores de máquinas de codificação recebiam a cada mês uma folha com as chaves, com as informações de como configurar suas máquinas em cada dia do mês. Um evidente risco de segurança havia com este sistema, pois bastava que os aliados interceptassem as folhas com as chaves que eles seriam capazes de ler as mensagens da Enigma. Por esta razão, as folhas com as chaves eram

extremamente bem guardadas e impressas com tinta solúvel. Se elas fossem capturadas pelos Aliados, os soldados alemães mergulhavam as folhas na água, limpando todas as informações.

Os alemães acreditavam que a segurança da Enigma residia no fato de que era impossível calcular rapidamente a chave dentre bilhões e bilhões de possibilidades, alteradas dia a dia. Enquanto os aliados não se apossassem da folha com as chaves, eles achavam que a sua comunicação permaneceria segura.

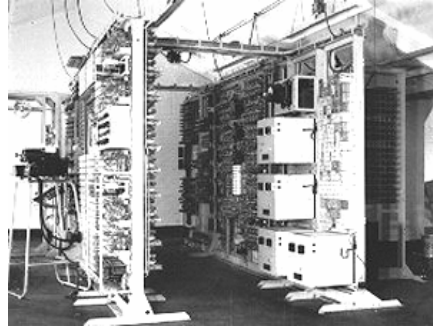
Eles não contavam com a inteligência e astúcia de Alan Turing e sua equipe que por volta de 1940 construíram o primeiro computador operacional para o serviço de inteligência britânico - uma gigantesca máquina que utilizava tecnologia de relés, feito especificamente para decifrar mensagens cifradas pela máquina Enigma.

Na verdade a história toda começou alguns anos antes. Por volta de 1930 os cientistas poloneses começaram secretamente a quebrar o código da Enigma e, pouco antes da Segunda Guerra começar, eles passaram estas informações para os governos da França e da Inglaterra.

Durante a Segunda Guerra, os submarinos alemães patrulhavam o Oceano Atlântico e eram o terror dos navios ingleses e americanos. Como vimos, para se comunicarem eles faziam o seguinte: os rotores e conexões da máquina Enigma eram mudados de acordo com o dia, seguindo um livro de códigos, a mensagem era então datilografada usando o teclado inferior da máquina. Cada letra datilografada fazia iluminar uma outra letra do teclado superior. A mensagem codificada era enviada então por rádio usando código Morse. Estas mensagens eram interceptadas em certas estações de escuta inglesas. Nestas estações trabalhavam equipes de operadores 24 horas por dia, que ouviam e listavam as mensagens, transformando o código Morse em letras.

Se apenas uma letra fosse decodificada errada, todo o trabalho de decifração daquela mensagem estaria perdido. Estas estações recebiam milhares de mensagens todos os dias.

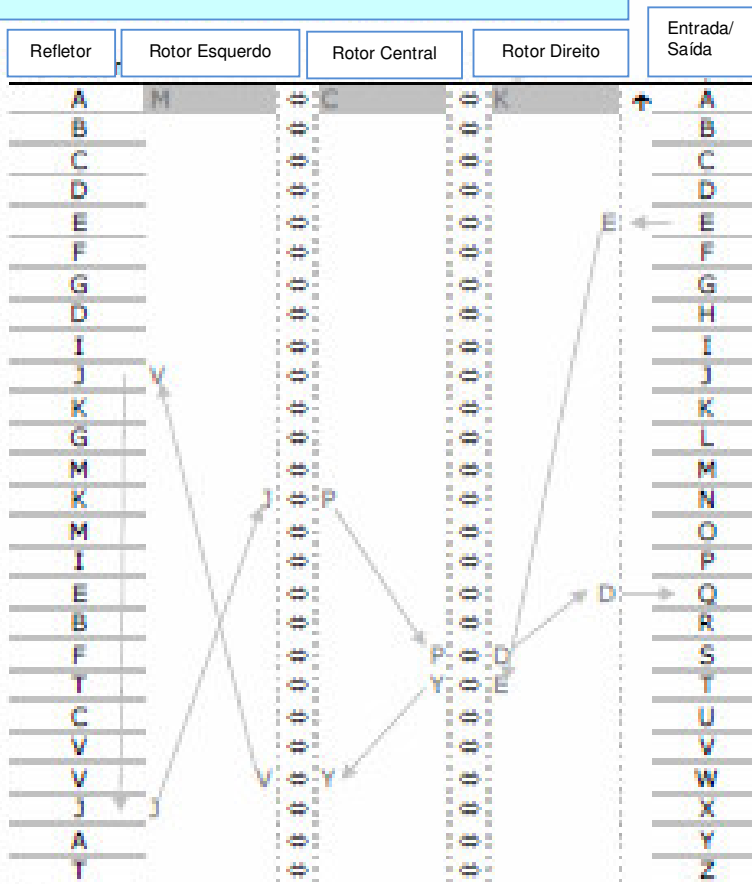
As mensagens interceptadas eram encaminhadas para uma central em Bletchley Park (na foto - localizada a 75 km de Londres), onde trabalhavam um grupo de pessoas especialmente escolhidas entre as mais inteligentes da Inglaterra. O trabalho era liderado por Alan Turing, que, como vimos, ajudou a arquitetar um dos primeiros computadores, usados para a quebra de códigos secretos. Esta central chegou a trabalhar com 7 mil pessoas, entre cientistas, operadores de máquinas e alimentadores de dados. Estas pessoas deviam manter segredo de suas atividades e trabalhavam em condições muito difíceis. A central de Bletchley Park recebia aproximadamente 3.000 mensagens codificadas a cada dia das estações de escuta. A única maneira de se quebrar o código do Enigma era comparar diferentes mensagens com outras para saber como os alemães tinham arranjado os rotores e conexões no dia em que foram enviadas. Deveriam descobrir em apenas duas horas qual das 158.000.000.000.000.000.000 possibilidades foi usada. Como algumas mensagens começavam com as mesmas palavras (por exemplo descrevendo as condições do tempo), surgiram pistas de como o resto da mensagem estava codificado. Utilizando máquinas eletro-mecânicas eles puderam decifrar algumas mensagens em menos de uma hora, mas quando os alemães passaram a usar máquinas Enigma com quatro rotores, o tempo necessário para decifrar mensagens subiu para dez meses.

Em 9 de maio de 1941 os aliados capturaram um submarino alemão e conseguiram apoderar-se de manuais de navegação e livros de códigos e sinais. Estes livros continham os códigos navais da máquina Enigma; para que os alemães não notassem imediatamente o conhecimento de seus códigos foi desenvolvida toda uma operação sigilosa envolvendo os que participaram da captura do submarino alemão. Cada uma das páginas do livro

de códigos foi fotografada e analisada pela equipe de pesquisadores do Bletchley Park, como um segredo de estado. Nesta época eles já podiam contar com um computador chamado Colossus (foto), projetado especialmente para decifrar mensagens secretas. Era um computador enorme que podia ler 5.000 letras por segundo através de um sistema fotoelétrico e todas as possíveis combinações de mensagens codificadas eram comparadas com as mensagens geradas pelas chaves criptográficas do Colossus, para revelar a configuração da máquina usada pelos alemães. Com este auxílio os ingleses conseguiram decifrar códigos gerados por máquinas Enigma com 12 rotores.

Em muitas ações a descoberta dos códigos alemães auxiliou na vitória dos aliados. Inclusive no dia D pode-se prever de antemão o tamanho e a localização das forças alemãs na Normandia.

O uso de máquinas durante a Segunda Grande Guerra alavancou o desenvolvimento de computadores muito mais poderosos que o Colossus e a criação de códigos muito mais complicados que o da máquina Enigma. Surgia assim a Era da Informática.

Para ver detalhadamente como a Enigma funcionava, acesse o site www.pbs.org/wgbh/nova/decoding/enigma.html. Há também um filme intitulado "Enigma", dirigido por Michael Apted que mostra a trama que envolveu a descoberta da decifração da máquina alemã.

Para compreender melhor o funcionamento da máquina Enigma, apresentaremos a seguir uma versão simulada, feita com papel. Apresentaremos também uma réplica em papel da máquina para visualizar seu aspecto externo.

Configuração Inicial: Escolha a ordem dos rotores, a seguir escolha a letra inicial de cada rotor e coloque-a na primeira linha da máquina, deslizando o rotor para cima.

Operação: Comece com a entrada na coluna mais à direita e caminhe para a esquerda até o Refletor, retorne então para a direita até encontrar a saída.

1. Se aparecer a seta, mova o rotor e seu vizinho da esquerda uma posição para cima. O rotor da direita sempre deve ser movido uma posição antes que cada letra seja codificada.
2. Localize a letra que você quer codificar na coluna da Entrada.
3. Veja a letra adjacente na coluna da direita do rotor da direita. Localize-a na coluna da esquerda deste mesmo rotor.
4. Passe para o rotor central e repita o processo.
5. Passe para o rotor da esquerda e repita o processo.
6. Observe qual letra aparece no Refletor e procure ainda no Refletor outra letra igual à que você encontrou.
7. Veja qual é a letra adjacente na coluna da esquerda do rotor da esquerda. Localize-a na coluna da direita deste mesmo rotor.
8. Passe para o rotor central e repita.
9. Passe para o rotor da direita e repita.
10. Observe qual é a letra correspondente na coluna da Saída. Esta será a letra codificada.
11. Repita para as demais letras da mensagem.

No exemplo descrito pelas setas cinzas usamos a ordem dos rotores I-II-III, as letras iniciais MCK e verificamos que a letra E é codificada pela letra Q.

Rotor I		Rotor II		Rotor III	
A	E	A	A	A	B
B	K	B	J	B	D
C	M	C	D	C	F
D	F	D	K	D	H
E	L	E	S	E	J
F	G	F	I	F	L
G	D	G	R	G	C
H	Q	H	U	H	P
I	V	I	X	I	R
J	Z	J	B	J	T
K	N	K	L	K	X
L	T	L	H	L	V
M	O	M	W	M	Z
N	W	N	T	N	N
O	Y	O	M	O	Y
P	H	P	C	P	E
Q	X	Q	Q	Q	I
R	U	R	G	R	W
S	S	S	Z	S	G
T	P	T	N	T	A
U	A	U	P	U	K
V	I	V	Y	V	M
W	B	W	F	W	U
X	R	X	V	X	S
Y	C	Y	O	Y	Q
Z	J	Z	E	Z	O
A	E	A	A	A	B
B	K	B	J	B	D
C	M	C	D	C	F
D	F	D	K	D	H
E	L	E	S	E	J
F	G	F	I	F	L
G	D	G	R	G	C
H	Q	H	U	H	P
I	V	I	X	I	R
J	Z	J	B	J	T
K	N	K	L	K	X
L	T	L	H	L	V
M	O	M	W	M	Z
N	W	N	T	N	N
O	Y	O	M	O	Y
P	H	P	C	P	E
Q	X	Q	Q	Q	I
R	U	R	G	R	W
S	S	S	Z	S	G
T	P	T	N	T	A
U	A	U	P	U	K
V	I	V	Y	V	M
W	B	W	F	W	U
X	R	X	V	X	S
Y	C	Y	O	Y	Q
Z	J	Z	E	Z	O

Estas três faixas devem ser recortadas e colocadas sobre o corpo da máquina

Como operar com a máquina Enigma de papel:

Como vimos anteriormente, a operação da máquina Enigma é muito simples: quando uma letra do teclado é pressionada, um contato mecânico é feito, permitindo que uma corrente elétrica chegue ao rotor posicionado no lado direito; este sinal passa então pelos três rotores, da direita para a esquerda. As ligações de fios dentro dos rotores produzem uma permutação das 26 letras do alfabeto. Depois da corrente passar da esquerda para a direita por dentro dos rotores, ela é refletida, através de uma permutação fixa e retorna novamente pelos rotores, agora da esquerda para a direita. Os 26 contatos são conectados a pequenas lâmpadas que iluminam a letra codificada em um painel superior ao teclado da máquina, assim que a tecla da letra original deixa de ser pressionada.

O rotor do lado direito roda uma posição quando uma nova tecla é pressionada, alterando deste modo a permutação das letras do alfabeto a cada apertar de tecla. Os outros rotores também giram, comandados pelo giro do primeiro rotor, como veremos em breve.

A máquina Enigma de papel é formada pelos seguintes componentes:

- corpo da máquina, onde serão inseridos os três rotores
- três faixas de papel que representam os rotores
- instruções

Os contatos entre os rotores são indicados por letras, à esquerda e à direita de cada faixa de papel. As conexões do refletor estão marcadas no corpo da máquina na coluna correspondente. As indicações das letras atuais dos rotores aparecem na primeira linha do corpo da máquina, na casa em cinza, elas serevm para indicar as posições iniciais dos rotores. As letras do teclado e as letras que são iluminadas no painel de saída, isto é, as entradas e saídas da máquina estão na coluna Entrada/Saída.

A montagem da máquina é muito simples; basta cortar as três faixas de papel que simulam os rotores e colocá-las sobre o corpo da máquina, na ordem desejada.

Para operar a máquina, vamos ilustrar com um exemplo, codificando a letra E a partir de uma configuração inicial que descreveremos abaixo:

- Primeiro escolhemos a ordem dos rotores e os colocamos sobre as colunas da máquina. Como exemplo, usaremos a ordem natural I, II, e III respectivamente nas colunas esquerda, central e direita.
- Ajustamos a posição inicial de cada rotor, deslizando-os verticalmente até que a letra que marca sua posição inicial esteja sobre a primeira linha (em cinza). Para exemplificar, escolheremos as letras inicias M, C e K, procurando-as nas colunas da esquerda dos rotores e colocando-as na primeira linha da máquina.
- O próximo passo é a rotação dos rotores. Isto é feito antes de codificar uma letra, antes mesmo da primeira inserção. O rotor do lado direito sempre sobe uma casa a cada apertar de tecla. Os rotores funcionam como um hodômetro, isto é, o movimento de um rotor à direita modifica o do seu vizinho do lado esquerdo. Mas cuidado!, isto <u>não</u> é realizado de modo cíclico como nos marcadores de quilometragem de automóveis, já que quando um rotor está numa determinada posição estratégica ele e seu vizinho da esquerda avançam juntos uma casa para cima. A razão é que os rotores não possuem um verdadeiro mecanismo de transporte (o famoso “vai um”), mas um mecanismo de encaixe do lado esquerdo que faz com que o rotor e seu vizinho se acoplem, girando juntos uma casa, mas só quando aparece no rotor da direita uma letra específica. Estas letras estão marcadas nas faixas dos rotores com uma seta. Quando esta seta aparecer em uma faixa, tanto o rotor desta faixa, como o seu vizinho à esquerda devem se movimentar uma posição para cima.

As conexões elétricas com cabos no painel frontal, por simplicidade, não são simuladas neste protótipo.

Veja o que ocorre para codificar a letra E, com a configuração inicial (I em M, II C e III em K): começamos colocando a letra E na entrada, subimos o rotor III uma casa e a letra E da entrada fica emparelhada com outra letra E do rotor III (na coluna da esquerda deste mesmo rotor), procure a letra E na coluna da esquerda, esta letra está associada à letra Y do rotor do meio, procure Y na coluna da esquerda do rotor do meio, ela está emparelhada com a letra V do rotor da esquerda, procure V na coluna da esquerda do rotor I e veja que ele está emparelhado com a letra J no refletor. Inicie o caminho inverso: J do rotor da esquerda associa-se a P do rotor do meio, que se associa a D do rotor da direita e que finalmente produz Q como saída. Assim a letra E fica codificada pela letra Q.

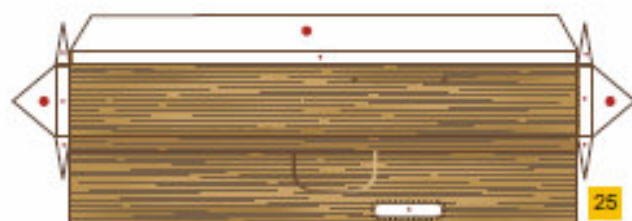
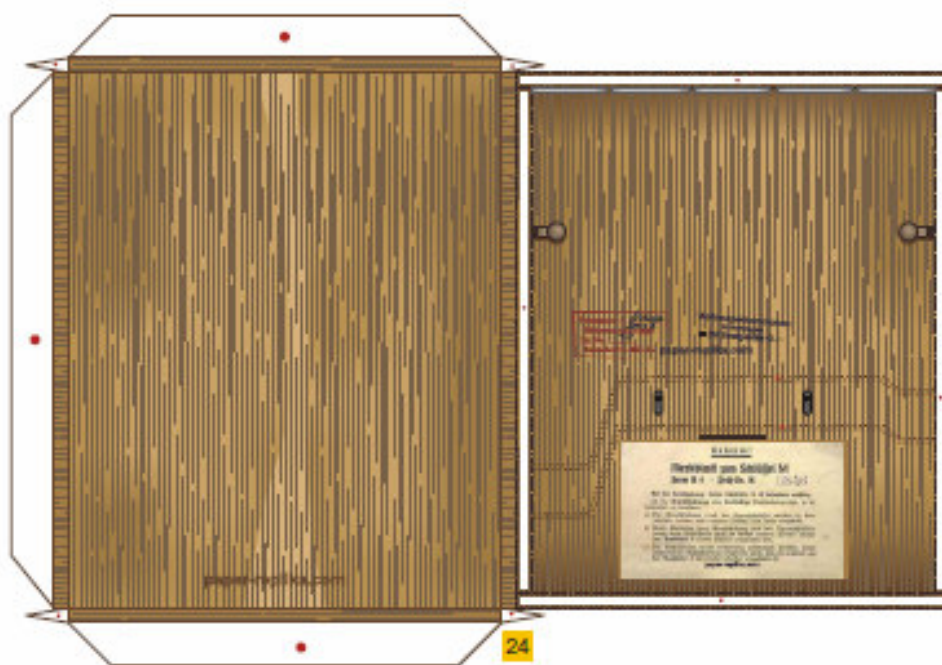
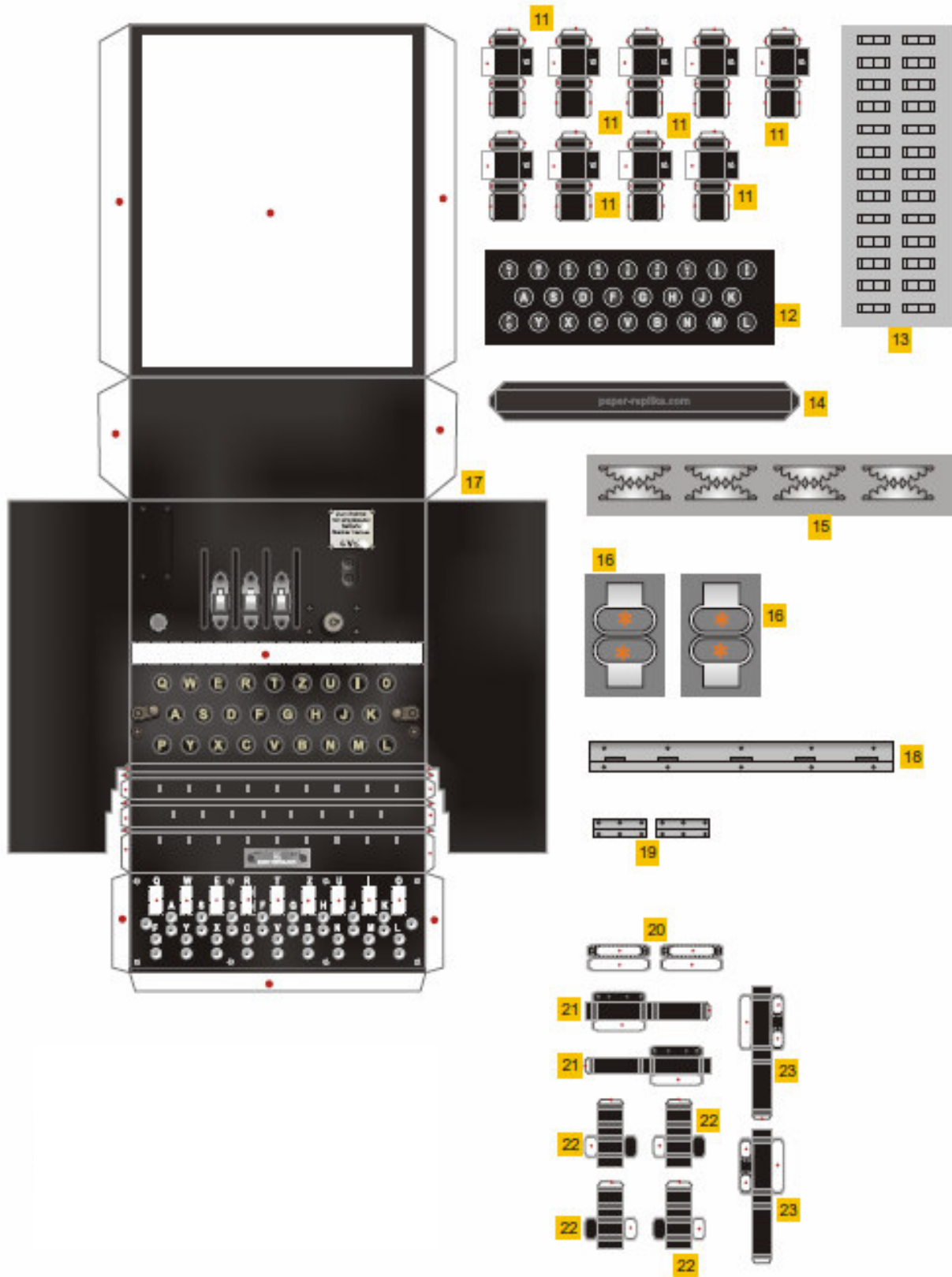
Para codificar outras letras, proceda da mesma maneira, não se esquecendo quando encontrar uma seta, movimente simultaneamente o rotor e seu vizinho da esquerda uma casa para cima.

Para decifrar uma mensagem basta colocar os rotores nas posições e letras iniciais com que foram codificados e proceder exatamente como se faz na codificação, seguindo o caminho inverso nos rotores, pois, como vimos, as chaves da máquina Enigma são simétricas.

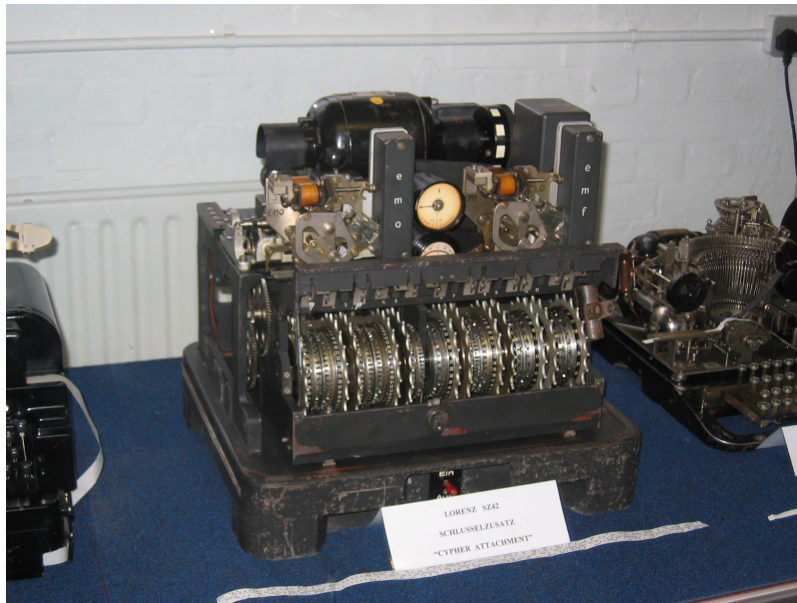
A seguir apresentamos uma réplica em papel da máquina Enigma. As instruções de montagem estão no site http://paper-replika.com/index.php?option=com_content&view=article&id=527:german-m4-naval-enigma-machine&catid=38&Itemid=200920

1
2
3
4
5
6
8
Klappe
schließen
9
7
10

24
25
26
27

11
12
13
14
15
16
17
18
19
20
21
22
23
paper-replika.com

ATIVIDADES COM A MÁQUINA DE LORENZ

A Máquina dos Generais Nazistas

Vamos estudar agora uma simplificação de uma outra máquina utilizada pelos alemães, conhecida como máquina de Lorenz, a fim de entender a matemática que está por trás dela. Veremos como a Teoria das Probabilidades foi essencial para quebrar o código produzido por tais máquinas.

A máquina de Lorenz modelo SZ 42 (Lorenz era o nome do fabricante) possuía 12 rotores que eram usados para embaralhar as letras de uma mensagem. Para criptografar mensagens, a máquina operava da seguinte maneira:

- As letras da mensagem eram transformadas em números binários.
- Cada um desses números binários era somado, através da aritmética binária, a outros números produzidos pela máquina, obtidos pela rotação das engrenagens.
- A mensagem criptografada era transformada em pulsos elétricos e enviada como uma mensagem telegráfica.

O procedimento para decifrar a mensagem era praticamente o mesmo que o descrito acima, apenas invertendo-se os passos. Vejamos isto com mais detalhes:

Transformando letras em números: Cada letra era transformada em um número binário de cinco algarismos, totalizando $2^5 = 32$ caracteres diferentes, de acordo com a seguinte tabela:

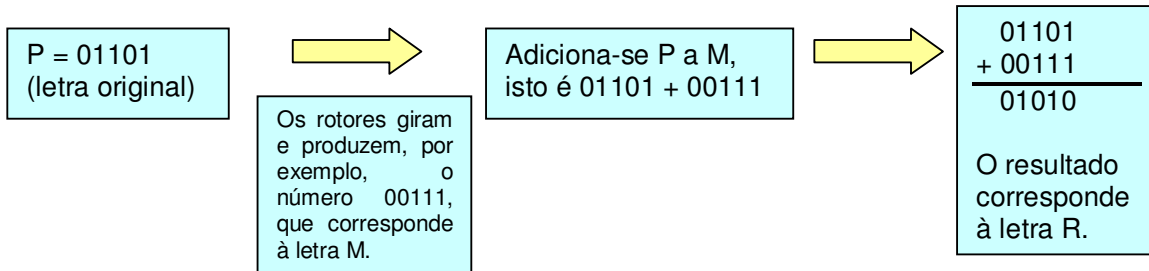
A	11000	B	10011	C	01110	D	10010	E	10000	F	10110	G	01011
H	00101	I	01100	J	11010	K	11110	L	01001	M	00111	N	00110
O	00011	P	01101	Q	11101	R	01010	S	10100	T	00001	U	11100
V	01111	W	11001	X	10111	Y	10101	Z	10001				
9	00100	8	11111	+	11011	4	01000	3	00010	/	00000		

Observe que, além das 26 letras usuais, seis outros símbolos eram utilizados ou como sinais de pontuação ou para controlar a impressão. O significado desses últimos seis símbolos não é o usual. Por exemplo, o algarismo 9 na verdade era usado para separar palavras (espaço em branco) e o símbolo + não denota a adição.

Se apenas esta codificação fosse feita, o código seria facilmente quebrado pelo método do estudo da frequência das letras, pois seria um código de César. Para evitar isto, quando uma letra era introduzida na máquina, os rotores giravam e doze novos números eram produzidos. Esses números eram somados ao número associado à letra e uma nova letra era produzida. A aritmética desta adição, entretanto, não é a usual; trata-se da adição binária:

$$0 + 0 = 0,\ \ 0 + 1 = 1,\ \ 1 + 0 = 1\ \text{ e }\ 1 + 1 = 0$$

Vejamos três exemplos:

1. Codificando a letra P com a letra chave M:

A letra P se transforma na letra R (pois P + M = 01101 + 00111 = 01010 = R)

2. Codificando uma letra com ela mesma:

A + A = 11000 + 11000 = 00000 = /, B + B = 10011 + 10011 = 00000 = /. . . .

Z + Z = 10001 + 10001 = 00000 = /.

Observe que o resultado é sempre o mesmo! Isto será explorado mais adiante para ajudar a quebrar o código da Máquina de Lorenz.

3. Codificando a palavra MASSA utilizando-se a chave WXYZA

Texto da mensagem	MASSA	→	00111	11000	10100	10100	11000
Chave	WXYZA	→	11001	10111	10101	10001	11000
Mensagem criptografada	KVTH/	←	11110	01111	00001	00101	00000

Como decifrar mensagens:

A adição binária possui ela mesma como inversa, isto é, se

Texto da mensagem + Chave = Mensagem criptografada

então

Mensagem criptografada + Chave = Texto da mensagem

Vejamos isto nos três exemplos anteriores:

1. Como P + M = 01101 + 00111 = 01010 = R, então R + M = 01010 + 00111 = 01101 = P.
2. Como A + A = 11000 + 11000 = 00000 = /, então A + / = 11000 + 00000 = 11000 = A. Analogamente para a repetição das demais letras do alfabeto.
3. Como MASSA + WXYZA = KVTH/, então KVTH/ + WXYZA = MASSA. De fato,

Mensagem criptografada	KVTH/	→	11110	01111	00001	00101	00000
Chave	WXYZA	→	11001	10111	10101	10001	11000
Texto da mensagem	MASSA	←	00111	11000	10100	10100	11000

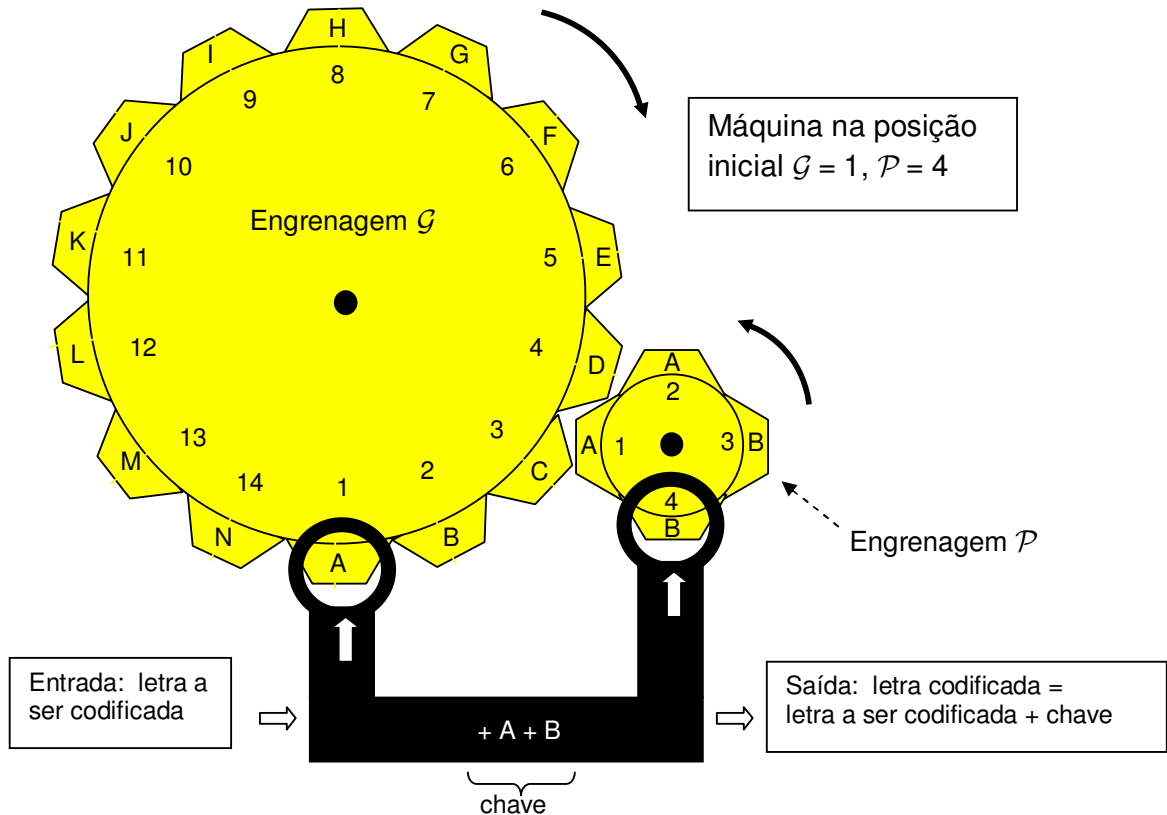
Para facilitar a tarefa de crifrar e decifrar, usamos a tabela abaixo com todas as 32 x 32 = 1024 possibilidades:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	9	8	+	4	3	/
A	/	G	F	R	4	C	B	Q	S	3	N	Z	8	K	+	Y	H	D	I	W	9	X	T	V	P	L	U	M	O	E	J	A
B	G	/	Q	T	O	H	A	F	8	L	P	J	S	Y	E	K	C	W	M	D	V	U	R	9	N	3	X	I	4	+	Z	B
C	F	Q	/	U	K	A	H	G	3	S	E	M	L	4	P	O	B	9	J	V	D	T	X	W	+	8	R	Z	Y	N	I	C
D	R	T	U	/	3	9	W	X	K	4	I	+	Y	S	Z	8	V	A	N	B	C	Q	G	H	M	O	F	P	L	J	E	D
E	4	O	K	3	/	N	+	Y	U	R	C	W	X	F	B	Q	P	J	9	Z	I	8	L	M	H	T	S	V	G	A	D	E
F	C	H	A	9	N	/	Q	B	J	I	4	8	Z	E	Y	+	G	U	3	X	R	W	V	T	O	M	D	L	P	K	S	F
G	B	A	H	W	+	Q	/	C	M	Z	Y	3	I	P	4	N	F	T	8	R	X	9	D	U	K	J	V	S	E	O	L	G
H	Q	F	G	X	Y	B	C	/	L	8	+	I	3	O	N	4	A	V	Z	9	W	R	U	D	E	S	T	J	K	P	M	H
I	S	8	3	K	U	J	M	L	/	F	D	H	G	R	V	T	Z	N	A	P	E	O	Y	+	W	Q	4	B	X	9	C	I
J	3	L	S	4	R	I	Z	8	F	/	9	B	Q	U	W	X	M	E	C	+	N	Y	O	P	V	G	K	H	T	D	A	J
K	N	P	E	I	C	4	Y	+	D	9	/	X	W	A	Q	B	O	S	R	8	3	Z	M	L	G	V	J	T	H	F	U	K
L	Z	J	M	+	W	8	3	I	H	B	X	/	C	V	R	9	S	O	Q	4	Y	N	E	K	U	A	P	F	D	T	G	L
M	8	S	L	Y	X	Z	I	3	G	Q	W	C	/	T	9	R	J	P	B	N	+	4	K	E	D	F	O	A	U	V	H	M
N	K	Y	4	S	F	E	P	O	R	U	A	V	T	/	H	G	+	I	D	M	J	L	8	Z	B	X	3	W	Q	C	9	N
O	+	E	P	Z	B	Y	4	N	V	W	Q	R	9	H	/	C	K	L	X	3	8	I	J	S	F	D	M	U	A	G	T	O
P	Y	K	O	8	Q	+	N	4	T	X	B	9	R	G	C	/	E	M	W	I	Z	3	S	J	A	U	L	D	F	H	V	P
Q	H	C	B	V	P	G	F	A	Z	M	O	S	J	+	K	E	/	X	L	U	T	D	9	R	4	I	W	3	N	Y	8	Q
R	D	W	9	A	J	U	T	V	N	E	S	O	P	I	L	M	X	/	K	G	F	H	B	Q	8	+	C	Y	Z	3	4	R
S	I	M	J	N	9	3	8	Z	A	C	R	Q	B	D	X	W	L	K	/	Y	4	+	P	O	T	H	E	G	V	U	F	S
T	W	D	V	B	Z	X	R	9	P	+	8	4	N	M	3	I	U	G	Y	/	Q	C	A	F	S	E	H	K	J	L	O	T
U	9	V	D	C	I	R	X	W	E	N	3	Y	+	J	8	Z	T	F	4	Q	/	B	H	G	L	P	A	O	M	S	K	U
V	X	U	T	Q	8	W	9	R	O	Y	Z	N	4	L	I	3	D	H	+	C	B	/	F	A	J	K	G	E	S	M	P	V
W	T	R	X	G	L	V	D	U	Y	O	M	E	K	8	J	S	9	B	P	A	H	F	/	C	I	4	Q	N	3	Z	+	W
X	V	9	W	H	M	T	U	D	+	P	L	K	E	Z	S	J	R	Q	O	F	G	A	C	/	3	N	B	4	I	8	Y	X
Y	P	N	+	M	H	O	K	E	W	V	G	U	D	B	F	A	4	8	T	S	L	J	I	3	/	9	Z	R	C	Q	X	Y
Z	L	3	8	O	T	M	J	S	Q	G	V	A	F	X	D	U	I	+	H	E	P	K	4	N	9	/	Y	C	R	W	B	Z
9	U	X	R	F	S	D	V	T	4	K	J	P	O	3	M	L	W	C	E	H	A	G	Q	B	Z	Y	/	+	8	I	N	9
8	M	I	Z	P	V	L	S	J	B	H	T	F	A	W	U	D	3	Y	G	K	O	E	N	4	R	C	+	/	9	X	Q	8
+	O	4	Y	L	G	P	E	K	X	T	H	D	U	Q	A	F	N	Z	V	J	M	S	3	I	C	R	8	9	/	B	W	+
4	E	+	N	J	A	K	O	P	9	D	F	T	V	C	G	H	Y	3	U	L	S	M	Z	8	Q	W	I	X	B	/	R	4
3	J	Z	I	E	D	S	L	M	C	A	U	G	H	9	T	V	8	4	F	O	K	P	+	Y	X	B	N	Q	W	R	/	3
/	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	9	8	+	4	3	/

Observe que esta matriz é simétrica devido à comutatividade da adição binária e também que na sua diagonal principal somente o símbolo / aparece.

Apresentaremos mais adiante um cilindro de criptografar que torna prática a consulta a esta tabela.

A Máquina de Lorenz com apenas duas engrenagens

Para entender como funciona a Máquina de Lorenz, vamos construir um modelo simplificado constituído de apenas um rotor, formado por duas engrenagens, uma grande ($\mathcal{G}$) com as 14 primeiras letras do alfabeto e outra pequena ($\mathcal{P}$) com quatro letras: dois A's e dois B's. Veja a figura:

As engrenagens giram a cada letra que é inserida na máquina e o resultado é a soma binária da letra que foi inserida com a soma das letras que aparecem na engrenagem $\mathcal{G}$ e na engrenagem $\mathcal{P}$. No caso ilustrado na figura, a letra original deve ser somada com A + B, resultando na letra criptografada. Para criptografar uma nova letra, as engrenagens giram uma posição ($\mathcal{G}$ no sentido horário e $\mathcal{P}$ no sentido contrário), e os mostradores da máquina exibem as letras B em $\mathcal{G}$ e A em $\mathcal{P}$. Deste modo B + A deve ser somado à segunda letra inserida. Para a terceira letra, novamente as engrenagens giram uma posição e assim sucessivamente até todas as letras terminarem.

Exemplo: Com a máquina na posição inicial $\mathcal{G}$ = 1, $\mathcal{P}$ = 4 (como na figura acima), podemos codificar a palavra SALA (consulte a tabela acima ou utilize o cilindro de Lorenz que aparecerá nas atividades práticas).

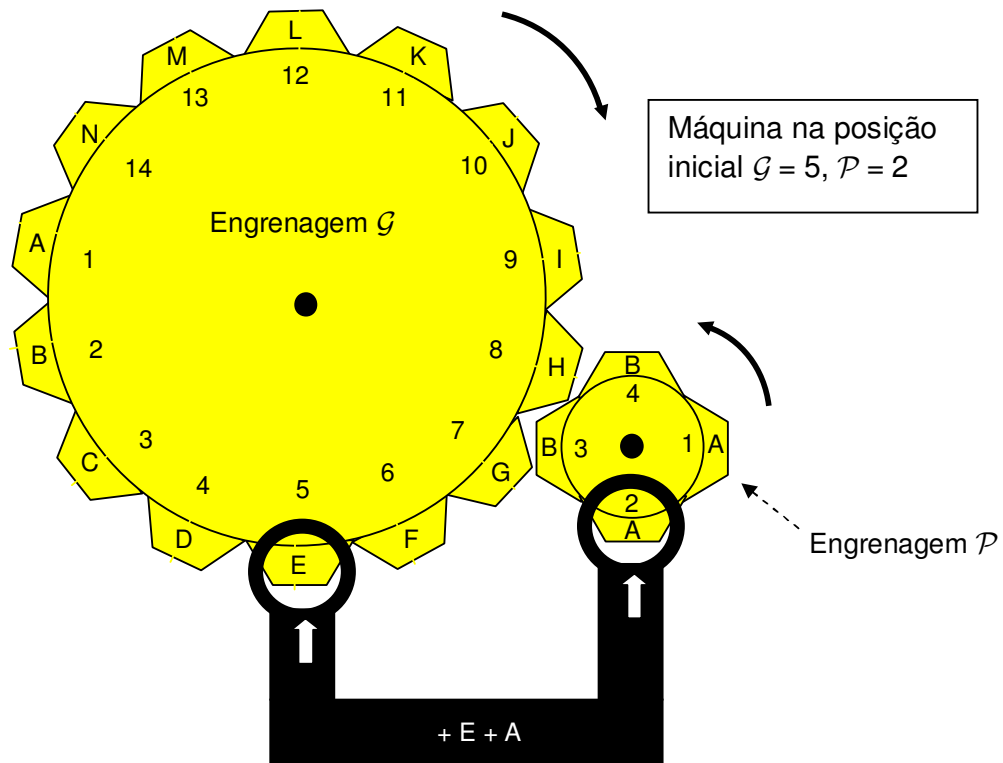
S + A + B = S + G = 8
A + B + A = A + G = B
L + C + A = L + F = 8
A + D + B = A + T = W

Ou seja, SALA se transforma em 8B8W. Observe que o símbolo 8 aparece duas vezes, mas criptografando letras diferentes; por isso o método da

contagem das frequências das letras usado para quebrar códigos no estilo de Júlio César não funciona com máquinas de Lorenz.

Mas esta repetição não vai causar dificuldades na decifração da mensagem? Não, pois a operação de soma binária é auto-invertível; veja:

8 + A + B = 8 + G = S
B + B + A = B + G = A
8 + C + A = 8 + F = L
W + D + B = W + T = A

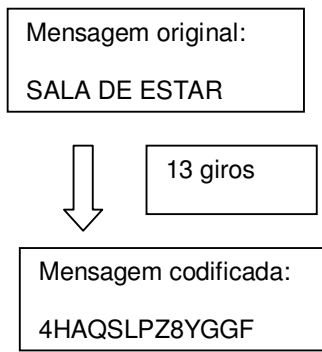
Exemplo: Com a máquina na posição inicial $\mathcal{G}$ = 5, $\mathcal{P}$ = 2 (como na figura abaixo), codifique a palavra SALA DE ESTAR (Lembre-se que o espaço em branco deve ser codificado como 9)

S + E + A = S + 4
A + F + B = A + H
L + G + B = L + A
A + H + A = A + Q
9 + I + A = 9 + S
D + J + B = D + L
E + K + B = E + P
9 + L + A = 9 + Z
E + M + A = E + 8
S + N + B = S + Y
T + A + B = T + G
A + B + A = A + G
R + C + A = R + F

Mensagem original:

SALA DE ESTAR

13 giros

Mensagem codificada:

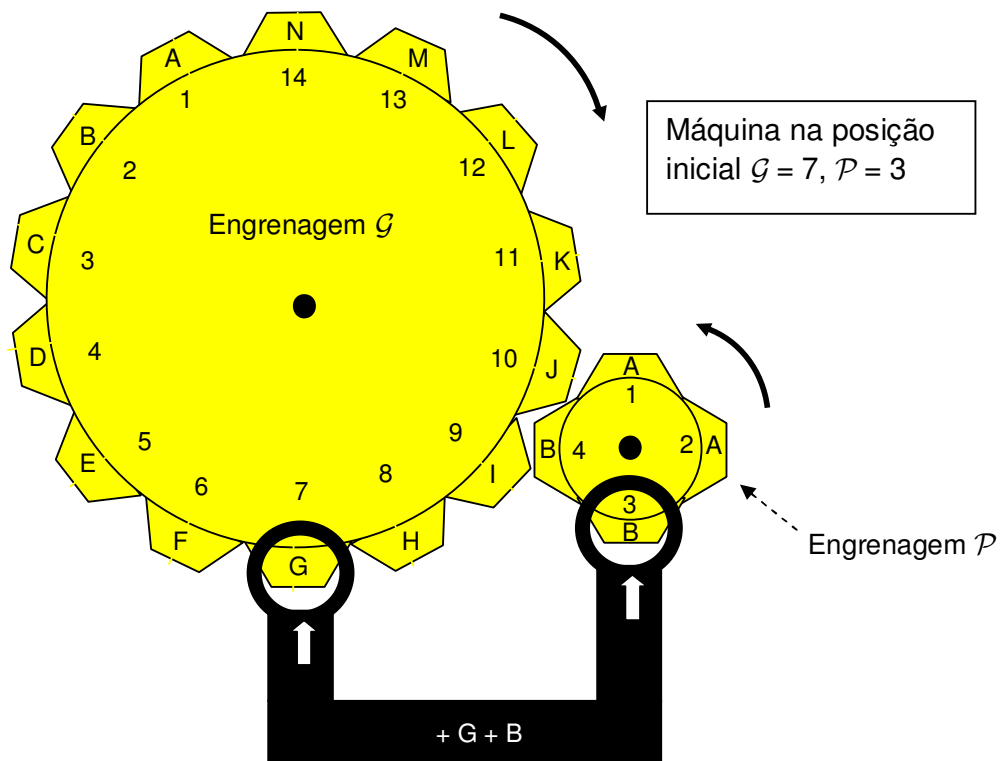
4HAQSLPZ8YGGF

É muito fácil decifrar uma mensagem se soubermos quais foram as posições iniciais das engrenagens $\mathcal{G}$ e $\mathcal{P}$. No nosso modelo simplificado existem apenas 14 x 4 = 56 possibilidades, mas na máquina de Lorenz verdadeira o número de possibilidades é enorme. Como fazer então para descobrir quais posições iniciais de $\mathcal{G}$ e $\mathcal{P}$ são as corretas, sem testar todas as possibilidades?

Um método para quebrar o código da Máquina de Lorenz:

Observando uma mensagem criptografada, é possível traçar pistas que nos permitem chegar às chaves (isto às posições iniciais de $\mathcal{G}$ e $\mathcal{P}$) da Máquina de Lorenz. Usamos para isto uma análise probabilística, a qual permite descobrir as chaves com uma boa margem de certeza, desde que a mensagem seja suficientemente longa.

Esta análise é baseada na observação de que a maioria das mensagens alemãs continha muitos pares de letras repetidas (por exemplo, espaços duplos entre as palavras). Vejamos um exemplo: a mensagem

9999A99ESFINGE99DISSE99DECIFRA99ME99OU99TE99DEVORO9999

será denotada pela letra $\mathcal{M}$. Vamos assumir que as posições iniciais das engrenagens sejam: $\mathcal{G}$ = 7 e $\mathcal{P}$ = 3.

Com essas chaves, a mensagem $\mathcal{M}$ se transforma em

(9+G+B)(9+H+B)(9+I+A)(9+J+A)(A+K+B)(9+L+B)(9+M+A)(E+N+A)(S+A+B)(F+B+B)(I+C+A)(N+D+A)(G+E+B)(E+F+B)(9+G+A)(9+H+A)(D+I+B)(I+J+B)(S+K+A)(S+L+A)(E+M+B)(9+N+B)(9+A+A)(D+B+A)(E+C+B)(C+D+B)(I+E+A)(F+F+A)(R+G+B)(A+H+B)(9+I+A)(9+J+A)(M+K+B)(E+L+B)(9+M+A)(9+N+A)(O+A+B)(U+B+B)(9+C+A)(9+D+A)(T+E+B)(E+F+B)(9+G+A)(9+H+A)(D+I+B)(E+J+B)(V+K+A)(O+L+A)(R+M+B)(O+N+B)(9+A+A)(9+B+A)(9+C+B)(9+D+B) =

(9+A)(9+F)(9+S)(9+3)(A+P)(9+J)(9+8)(E+K)(S+G)(F+/)(I+F)(N+R)(G+Q)(E+H)(9+B)(9+Q)(D+8)(I+L)(S+N)(S+Z)(E+S)(9+Y)(9+/)(D+G)(E+Q)(C+T)(I+4)(F+C)(R+A)(A+F)(9+S)(9+3)(M+P)(E+J)(9+8)(9+K)(O+G)(U+/)(9+F)(9+R)(T+O)(E+H)(9+B)(9+Q)(D+8)(E+L)(V+N)(O+Z)(R+S)(O+Y)(9+/)(9+G)(9+Q)(9+T) =

UDENYK+C8FJIFYXWPHDH9Z9WPV9ADCENRR+J4UDCBYXWPWLDKF9VWH,

que será denotada pela letra $\mathcal{C}$. Esta mensagem, assim como a original, tem 54 caracteres.

Suponhamos agora que as posições iniciais das engrenagens (as chaves) **não** sejam conhecidas e que só tenhamos em mãos a mensagem criptografada $\mathcal{C}$. Será possível decifrar a mensagem? Podemos, a partir dela, descobrir as chaves, isto é, as posições iniciais de $\mathcal{G}$ e $\mathcal{P}$?

O método a seguir permitirá tentativamente descobrir essas chaves, com base no estudo de probabilidades, sem recorrer à listagem completa de todas as possibilidades.

Teste:

a) Primeiramente transformamos a mensagem criptografada $\mathcal{C}$ em uma mensagem modificada, denotada por $|\mathcal{C}|$, obtida somando-se o primeiro ao segundo caractere de $\mathcal{C}$, a seguir o segundo com o terceiro e assim por diante até terminar a todos os componentes da mensagem.

   No exemplo que estamos acompanhando

$\mathcal{C}$ = UDENYK+C8FJIFYXWPHDH9Z9WPV9ADCENRR+J4UDCBYXWPWLDKF9VWH

e a mensagem modificada é:

$|\mathcal{C}|$ =
(U+D)(D+E)(E+N)(N+Y)(Y+K)(K++)(++C)(C+8)(8+F)(F+J)(J+I)(I+F)(F+Y)(Y+X)(X+W)
(W+P)(P+H)(H+D)(D+H)(H+9)(9+Z)(Z+9)(9+W)(W+P)(P+V)(V+9)(9+A)(A+D)(D+C)
(C+E)(E+N)(N+R)(R+R)(R++)(++J)(J+4)(4+U)(U+D)(D+C)(C+B)(B+Y)(Y+X)(X+W)
(W+P) (P+W)(W+L)(L+D)(D+K)(K+F)(F+9)(9+V)(V+W)(W+H) =

$|\mathcal{C}|$ = C3FBGHYZLIFJO3C S4XXTYYQS3GURU KFI/ZTDSCUQN3CSSE+I4DGFU

Observe que $|\mathcal{C}|$ tem 53 caracteres, um a menos que $\mathcal{C}$. (Não confundir o símbolo + de operação, com o mesmo símbolo usado na criptografia).

b) Adicionamos $|\mathcal{C}|$ com $|\mathcal{G}_i|$, i = 1,...,14 e contamos o número de "/" em cada uma dessas 14 mensagens. Aquela que apresentar o maior número de "/" provavelmente será a que fornecerá a posição inicial $i = i_0$ da engrenagem $\mathcal{G}$.

Para cada uma das 14 configurações diferentes da engrenagem $\mathcal{G}$, temos:

$\mathcal{G}_1$ = ABCDEFGHIJKLMNA... → $|\mathcal{G}_1|$ = GQU3NQCLF9XCTK...
$\mathcal{G}_2$ = BCDEFGHIJKLMNAB... → $|\mathcal{G}_2|$ = QU3NQCLF9XCTKG...
$\mathcal{G}_3$ = CDEFGHIJKLMNABC... → $|\mathcal{G}_3|$ = U3NQCLF9XCTKGQ...
$\mathcal{G}_4$ = DEFGHIJKLMNABCD... → $|\mathcal{G}_4|$ = 3NQCLF9XCTKGQU...
$\mathcal{G}_5$ = EFGHIJKLMNABCDE... → $|\mathcal{G}_5|$ = NQCLF9XCTKGQU3...
$\mathcal{G}_6$ = FGHIJKLMNABCDEF... → $|\mathcal{G}_6|$ = QCLF9XCTKGQU3N...
$\mathcal{G}_7$ = GHIJKLMNABCDEFG... → $|\mathcal{G}_7|$ = CLF9XCTKGQU3NQ...
$\mathcal{G}_8$ = HIJKLMNABCDEFGH... → $|\mathcal{G}_8|$ = LF9XCTKGQU3NQC...
$\mathcal{G}_9$ = IJKLMNABCDEFGHI... → $|\mathcal{G}_9|$ = F9XCTKGQU3NQCL...
$\mathcal{G}_{10}$ = JKLMNABCDEFGHIJ... → $|\mathcal{G}_{10}|$ = 9XCTKGQU3NQCLF...
$\mathcal{G}_{11}$ = KLMNABCDEFGHIJK... → $|\mathcal{G}_{11}|$ = XCTKGQU3NQCLF9...
$\mathcal{G}_{12}$ = LMNABCDEFGHIJKL... → $|\mathcal{G}_{12}|$ = CTKGQU3NQCLF9X...
$\mathcal{G}_{13}$ = MNABCDEFGHIJKLM... → $|\mathcal{G}_{13}|$ = TKGQU3NQCLF9XC...
$\mathcal{G}_{14}$ = NABCDEFGHIJKLMN... → $|\mathcal{G}_{14}|$ = KGQU3NQCLF9XCT...

e adicionamos $|\mathcal{C}|$ com $|\mathcal{G}_i|$, i = 1,...,14. Na verdade estas somas não precisam ser realizadas efetivamente; o que nos interessa é o número de "/" em cada caso e isto pode ser obtido observando se os caracteres de cada fator são iguais.

$|\mathcal{C}| + |\mathcal{G}_1|$ = (C3FBGHYZLIFJO3CS4XXTYYQS3GURUKFI/ZTDSCUQ N3CSSE+I4DGFU) +
(GQU3NQCLF9XCTKGQU3NQCLF9XCTKGQU3NQCLF9XC TKGQU3NQCLF9X)

(não aparecem caracteres repetidos ocupando a mesma posição nos fatores; portanto no resultado nenhum “/” aparecerá)

$|\mathcal{C}| + |\mathcal{G}_2|$ = (C3FBGHYZLIFJO3CS4XXTYYQS3GURUKFI/ZTDSCUQN3CSSE+I4DGFU) +
(QU3NQCLF9XCTKGQU3NQCLF9XCTKGQU3NQCLF9XCTKGQU3NQCLF9XC)
(nenhum “/”)

$|\mathcal{C}| + |\mathcal{G}_3|$ = (C**3**FBGHYZLIFJO3CS4XXTYYQS3GUR**U**KFI/ZTDS**C**UQN3CSSE+I4DGFU) +
(U**3**NQCLF9XCTKGQU3NQCLF9XCTKGQ**U**3NQCLF9X**C**TKGQU3NQCLF9XCT)
(três “/” – em negrito as letras repetidas na mesma posição)

$|\mathcal{C}| + |\mathcal{G}_4|$ = (C3FBGHYZLIFJO3CS4XXTYYQS3**G**URUKFI/ZTDSCUQN3CSSE+I4DGFU) +
(3NQCLF9XCTKGQU3NQCLF9XCTK**G**QU3NQCLF9XCTKGQU3NQCLF9XCTK)
(apenas um “/”)

$|\mathcal{C}| + |\mathcal{G}_5|$ = (C3FBGHYZLIFJO**3**CS4XXTYYQS3G**U**RUKFI/ZTDSCU**Q**N**3**CSSE+I4DGFU) +
(NQCLF9XCTKGQU**3**NQCLF9XCTKGQ**U**3NQCLF9XCTKG**Q**U**3**NQCLF9XCTKG)
(três “/”)

$|\mathcal{C}| + |\mathcal{G}_6|$ = (C3FBGHYZLIFJO3CS4XXTYYQS3GURUKFI/ZTDSCUQN3CSSE+I4DGFU) +
(QCLF9XCTKGQU3NQCLF9XCTKGQU3NQCLF9XCTKGQU3NQCLF9XCTKGQ)
(nenhum “/”)

$|\mathcal{C}| + |\mathcal{G}_7|$ = (**C**3**F**BGHYZLIFJO3**C**S4X**X**TYYQS3GURUK**F**I/Z**T**DSC**U**Q**N**3**C**SSE+I4D**G**F**U**) +
(**C**L**F**9XCTKGQU3NQ**C**LF9**X**CTKGQU3NQCL**F**9XC**T**KGQ**U**3**N**Q**C**LF9XCTK**G**Q**U**)
= /G/XUGSV3ZRAH8/QKB/VSGFLKLJXDX/4X8/I8B/8/8/Q3SI3LI/G/
(11 caracteres “/”, neste caso valeu a pena fazer a soma, pois trata-se da posição correta)

$|\mathcal{C}| + |\mathcal{G}_8|$ = (C3FBGHYZLIFJO3CS4**X**X**T**YY**Q**S**3**GURUKFI/ZTDSCUQN3CSSE+I4DGFU) +
(LF9XCTKGQU3NQCLF9**X**C**T**KG**Q**U**3**NQCLF9XCTKGQU3NQCLF9XCTKGQU3)
(três “/”)

$|\mathcal{C}| + |\mathcal{G}_9|$ = (C3FBGHYZLIFJO3CS4XXTYYQS3GURUKFI/ZTDSCU**Q**N3CSSE+I4DGFU) +
(F9XCTKGQU3NQCLF9XCTKGQU3NQCLF9XCTKGQU3N**Q**CLF9XCTKGQU3N)
(um “/”)

$|\mathcal{C}| + |\mathcal{G}_{10}|$ = (C3FBGHYZLIFJO3CS4XXTYYQS3GURUKFI/ZTDSCUQN3CSSE+I4DGFU) +
(9XCTKGQU3NQCLF9XCTKGQU3NQCLF9XCTKGQU3NQCLF9XCTKGQU3NQ)
(nenhum “/”)

$|\mathcal{C}| + |\mathcal{G}_{11}|$ = (C3FB**G**HYZLIFJO3CS4XXTYYQS3GURUKFI/ZTDSCUQN3CSSE+I4DGFU) +
(XCTK**G**QU3NQCLF9XCTKGQU3NQCLF9XCTKGQU3NQCLF9XCTKGQU3NQC)
(um “/”)

$|\mathcal{C}| + |\mathcal{G}_{12}|$ = (**C**3FBGHYZLIFJO3**C**S4XXTYY**Q**S3GURUKFI/ZTDS**C**UQN3**C**SSE+I4DGFU) +
(**C**TKGQU3NQCLF9X**C**TKGQU3N**Q**CLF9XCTKGQU3NQ**C**LF9X**C**TKGQU3NQCL)
(cinco “/”)

$|\mathcal{C}| + |\mathcal{G}_{13}|$ = (C3FBGHYZLI**F**JO3CS4XXTYYQS3GURU**K**FI/ZTDSCUQN3CSSE+I4DGFU) +
(TKGQU3NQCL**F**9XCTKGQU3NQCLF9XCT**K**GQU3NQCLF9XCTKGQU3NQCLF)
(dois “/”)

$|\mathcal{C}| + |\mathcal{G}_{14}|$ = (C3FBGHYZLIFJO3CS4XXTYYQS3GURUKFI/ZTDSCUQN3CSSE+I4DGFU) +
(KGQU3NQCLF9XCTKGQU3NQCLF9XCTKGQU3NQCLF9XCTKGQU3NQCLF9)
(nenhum “/”)

Após contar o número de "/" em cada uma das mensagens acima, selecionamos aquela que apresentar o maior número de "/". Ela provavelmente será a que fornecerá a posição inicial da engrenagem $\mathcal{G}$. No caso em questão a posição mais favorável é $\mathcal{G}_7$, a sétima posição da engrenagem $\mathcal{G}$.

c) Testamos agora $\mathcal{G}_7$ com as 4 possíveis posições de $\mathcal{P}$:

(j=1) $\mathcal{G}_7$ com $\mathcal{P}_1$:

UDENYK+C8FJIFYXWPHDH9Z9WPV9ADCENRR+J4UDCBYXWPWLDKF9VWH
+
GHIJKLMNABCDEFGHIJKLMNABCDEFGHIJKLMNABCDFGHIJKLMNABCDE
+
AABBAABBAABBAABBAABBAABBAABBAABBAABBAABBAABBAABBAABBAA

VVVVBVV+... (mensagem sem sentido, não deve ser esta a posição correta)

(j=2) $\mathcal{G}_7$ com $\mathcal{P}_2$:

UDENYK+C8FJIFYXWPHDH9Z9WPV9ADCENRR+J4UDCBYXWPWLDKF9VWH
+
GHIJKLMNABCDEFGHIJKLMNABCDEFGHIJKLMNABCDFGHIJKLMNABCDE
+
ABBAABBAABBAABBAABBAABBAABBAABBAABBAABBAABBAABBAABBAAB

V9V9B9V... (mensagem sem sentido, não deve ser esta a posição correta)

(j=3) $\mathcal{G}_7$ com $\mathcal{P}_3$:

UDENYK+C8FJIFYXWPHDH9Z9WPV9ADCENRR+J4UDCBYXWPWLDKF9VWH
+
GHIJKLMNABCDEFGHIJKLMNABCDEFGHIJKLMNABCDFGHIJKLMNABCDE
+
BBAABBAABBAABBAABBAABBAABBAABBAABBAABBAABBAABBAABBAABB

9999**A**99**ESFINGE**99**DISSE**99**DECIFRA**99**ME**99**OU**99**TE**99**DEVORO**9999

(j=4) $\mathcal{G}_7$ com $\mathcal{P}_4$:

UDENYK+C8FJIFYXWPHDH9Z9WPV9ADCENRR+J4UDCBYXWPWLDKF9VWH
+
GHIJKLMNABCDEFGHIJKLMNABCDEFGHIJKLMNABCDFGHIJKLMNABCDE
+
BAABBAABBAABBAABBAABBAABBAABBAABBAABBAABBAABBAABBAABBA

9V9VAV9... (mensagem sem sentido, não deve ser esta a posição correta)

Conclusão: A partir de uma mensagem codificada suficientemente longa e sabendo-se que a mensagem original possui muitos caracteres repetidos, podemos encontrar as posições iniciais das engrenagens e decifrá-la.

Porque o método descrito acima funciona? Para responder a esta pergunta, precisaremos estudar os princípios básicos das probabilidades.

Noções de Teoria das Probabilidades

A Teoria das Probabilidades estuda modelos que descrevem fenômenos aleatórios (*alea* em latim significa sorte, acaso). Sua origem é relativamente recente e esteve ligada aos jogos de azar; por isto, os primeiros estudos probabilísticos descreviam situações em que os eventos eram igualmente prováveis (por exemplo, a chance de sair cara ou coroa no lançamento de uma moeda é a mesma se ela for honesta).

> Intuitivamente a probabilidade está diretamente relacionada com a frequência que um evento se repete, quando o experimento subjacente é realizado um número muito grande (tendendo ao infinito) de vezes. Esta conexão entre a Probabilidade e a Estatística é fundamental e pode ser tornada rigorosa a través de um teorema, conhecido como a "**Lei dos Grandes Números**". Neste texto estas idéias serão utilizadas sem formalismos.

Quando realizamos um experimento constituído de eventos elementares igualmente prováveis, devemos selecionar com precisão qual é o conjunto de todos os casos possíveis (conhecido como *Espaço Amostral* e usualmente denotado pela letra grega Ω). Devemos também escolher dentro de Ω um subconjunto A que nos interessa ao estudo (estes subconjuntos são chamados de *eventos*) e assim definir a probabilidade de ocorrer A como quociente

$$P(A) = \frac{\text{número de casos favoráveis}}{\text{número de casos possíveis}} = \frac{\#(A)}{\#(\Omega)}$$

em que # (A) denota o número de elementos do conjunto A.

Se A e B são dois eventos de um espaço amostral Ω, como

$$P(A \cup B) = \frac{\#(A)}{\#(\Omega)} + \frac{\#(B)}{\#(\Omega)} - \frac{\#(A \cap B)}{\#(\Omega)}$$

então $P(A \cup B) = P(A) + P(B) - P(A \cap B)$. Assim, se dois eventos são **disjuntos**, então P(AUB) = P(A) + P(B).

Dizemos que dois eventos são **independentes** se $P(A \cap B) = P(A) \times P(B)$; isto intuitivamente equivale a dizer que a ocorrência de A em nada influencia a ocorrência de B.

Exemplo 1: Qual é a probabilidade de se obter o "/" quando somamos dois caracteres quaisquer da Máquina de Lorenz?

O espaço amostral é formado por 32 x 32 duplas de caracteres e somente 32 dessas duplas (as que possuem o primeiro e o segundo fatores repetidos) produzirão, quando somarmos seus fatores, o símbolo "/". Assim:

$$P(/) = \frac{\text{número de casos favoráveis}}{\text{número de casos possíveis}} = \frac{32}{32\text{x } 32} = \frac{1}{32} \cong 3\%$$

Exemplo 2: Qual é a probabilidade de um símbolo da mensagem modificada $|\mathcal{P}_1|$ ser igual a / , quando giramos um grande número de vezes a engrenagem $\mathcal{P}$?

Se a engrenagem $\mathcal{P}$ é girada um grande número de vezes a partir da posição inicial j =1, obteremos a sequência AABBAABB..., o que produz a mensagem modificada $|\mathcal{P}_1|$ =/G/G/G/G... Logo

$$P(|\mathcal{P}_1| = /) = \frac{1}{2}$$

Porque o teste com a máquina de Lorenz funciona:

TESTE

a) Transformamos a mensagem criptografada $\mathcal{C}$ em uma mensagem modificada, denotada por $|\mathcal{C}|$, obtida somando-se o primeiro ao segundo caractere de $\mathcal{C}$, a seguir o segundo com o terceiro e assim por diante até terminar a todos os componentes da mensagem.

b) Adicionamos $|\mathcal{C}|$ com $|\mathcal{G}_i|$, i = 1,...,14 e contamos o número de "/" em cada uma dessas 14 mensagens. Aquela que apresentar o maior número de "/" provavelmente será a que fornecerá a posição inicial $i = i_0$ da engrenagem $\mathcal{G}$.

d) Testamos agora $\mathcal{G}_i$ com $i = i_0$ com as 4 possíveis posições iniciais de $\mathcal{P}_j$, j =1,2,3,4, até encontrar uma mensagem que faça sentido.

Faremos nosso raciocínio sobre a mensagem

$\mathcal{M}$ = 9999A99ESFINGE99DISSE99DECIFRA99ME99OU99TE99DEVORO9999

mas o raciocínio é geral e se aplica a outras mensagens suficientemente longas. Usamos as posições iniciais $\mathcal{G}$ = 7, $\mathcal{P}$ = 3 para obter a mensagem criptografada:

$\mathcal{C}$ = UDENYK+C8FJIFYXWPHDH9Z9WPV9ADCENRR+J4UDCBYXWPWLDKF9VWH

Vamos dividir nossa análise em dois casos:

CASO 1: A posição inicial da engrenagem $\mathcal{G}$ é a errada, isto é, $i_0 \neq 7$. Não sabemos isto de antemão, mas, se de fato esta engrenagem estivesse na posição incorreta o número de caracteres "/" em $|\mathcal{C}| + |\mathcal{G}_i|$, deveria ser estatisticamente (e probabilisticamente) muito baixo. De fato,

Se em alguma posição da mensagem $|\mathcal{C}| + |\mathcal{G}_i|$ aparecer o caractere /, então os símbolos nesta posição devem ser iguais, mas a probabilidade disto ocorrer já foi calculada no Exemplo 1:

$$P(|\mathcal{C}| + |\mathcal{G}_i| = /) = \frac{1}{32} \cong 3\%$$

uma probabilidade baixa.

CASO 2: A posição inicial da engrenagem $\mathcal{G}$ é a correta, isto é, $i_0 = 7$. Nada sabemos ainda sobre a posição inicial $\mathcal{P}_j$; ela será testada no final.

Como

$$\mathcal{C} = \mathcal{M} + \mathcal{G}_i + \mathcal{P}_j, \text{ para } i = i_0 \text{ e para algum } j \in \{1,2,3,4\}$$

então $|\mathcal{C}| = |\mathcal{M}| + |\mathcal{G}_i| + |\mathcal{P}_j|$, ou seja $|\mathcal{C}| + |\mathcal{G}_i| = |\mathcal{M}| + |\mathcal{P}_j|$ (lembre-se a adição binária é auto-invertível).

Voltemos ao nosso teste: se em alguma posição da mensagem $|\mathcal{C}| + |\mathcal{G}_i|$ aparecer o caractere "/", então o mesmo deve ocorrer com $|\mathcal{M}| + |\mathcal{P}_j|$. Simbolicamente:

$$|\mathcal{C}| + |\mathcal{G}_i| = / \Rightarrow |\mathcal{M}| + |\mathcal{P}_j| = / \Rightarrow |\mathcal{M}| = |\mathcal{P}_j|$$

Mas existem apenas 4 possibilidades para $\mathcal{P}_j$:

$\mathcal{P}_1$: AABBAABB... $\Rightarrow |\mathcal{P}_1|$ = /G/G/G/G....
$\mathcal{P}_2$: ABBAABBA... $\Rightarrow |\mathcal{P}_2|$ = G/G/G/G/....

$\mathcal{P}_3$: BBAABBAA... $\Rightarrow |\mathcal{P}_3|$ = /G/G/G/G....

$\mathcal{P}_4$: BAABBAAB... $\Rightarrow |\mathcal{P}_4|$ = G/G/G/G/....

Assim, para que algum caractere de $|\mathcal{M}|$ seja igual a algum caractere de $\mathcal{P}_j$, este símbolo deve ser fatalmente / ou G.

Aqui entra o grande erro de se transmitir mensagens com muitas repetições: a chance de se obter muitos "/" em $|\mathcal{M}|$ é grande, o que nos dá pistas de como foram escolhidas as posições originais da máquina!

Vejamos isto com mais detalhes: se algum caractere de $|\mathcal{M}|$ for igual a algum caractere de $\mathcal{P}_j$, então, só existem duas possibilidades:

- esse caractere é G ou
- esse caractere é /

A probabilidade de ocorrer a primeira situação será indicada por P ($|\mathcal{M}|$ = G) e a segunda por P ($|\mathcal{M}|$ = /). Os dois eventos acima são disjuntos e portanto

$$P(|\mathcal{C}| + |\mathcal{G}_i| = /) = P(|\mathcal{M}| = |\mathcal{P}_j|) = P\left(|\mathcal{M}| = G \text{ e } |\mathcal{P}_j| = G\right) + P\left(|\mathcal{M}| = / \text{ e } (|\mathcal{P}_j| = /\right)$$

Ora, os eventos são também independentes, logo

$P\left(|\mathcal{M}| = G \text{ e } |\mathcal{P}_j| = G\right) = P\left(|\mathcal{M}| = G\right) . P\left(|\mathcal{P}_j| = G\right) = (1/32). (1/2) = (1/64)$

Conforme Exemplos 1 e 2, vistos anteriormente.

e, para calcular

$$P\left(|\mathcal{M}| = / \text{ e } (|\mathcal{P}_j| = /\right) = P\left(|\mathcal{M}| = /\right) . P\left(|\mathcal{P}_j| = /\right) = (1/2). P\left(|\mathcal{M}| = /\right)$$

devemos fazer uma previsão da frequência de repetições de letras na mensagem original (isto é claro, depende da língua e do tipo de mensagem que se está enviando), já que a probabilidade de encontrarmos "/" na mensagem modificada $|\mathcal{M}|$ está vinculada diretamente ao número de repetições de caracteres na mensagem original $\mathcal{M}$. Usando nossa mensagem

$\mathcal{M}$ = 9999A99ESFINGE99DISSE99DECIFRA99ME99OU99TE99DEVORO9999

vemos que existe 12 repetições em 54 letras e assim uma boa estimativa para $P\left(|\mathcal{M}| = /\right)$ é (12/54) = (2/9), aproximadamente 22%. Na verdade, como conhecemos a mensagem original, podemos refinar esta estimativa, escrevendo explicitamente $|\mathcal{M}|$ e contando os caracteres "/" (o resultado será 14/53, aproximadamente 26%).

Assim,

$$P\left(|\mathcal{C}| + |\mathcal{G}_i| = /\right) = P\left(|\mathcal{M}| = |\mathcal{P}_j|\right) =$$

$$P\left(|\mathcal{M}| = G \text{ e } |\mathcal{P}_j| = G\right) + P\left(|\mathcal{M}| = / \text{ e } (|\mathcal{P}_j| = /\right) =$$

$$= \frac{1}{64} + \frac{1}{2}.\frac{14}{53} \cong 0{,}147$$

Isto significa que, nas condições descritas acima, quando a posição da engrenagem $\mathcal{G}$ é a correta, temos perto de 15% de que um caractere de $|\mathcal{C}| + |\mathcal{G}_i|$ seja "/", contra 3% do mesmo ocorrer se $\mathcal{G}$ estiver em alguma posição errada! No nosso exemplo, podemos fazer uma estimativa do número de "/" esperados nos dois casos:

- Em uma posição errada, espera-se que apareçam 3% de 53 = 1,5 caracteres "/" na mensagem (encontramos $\mathcal{G}_1 \to 0$, $\mathcal{G}_2 \to 0$, $\mathcal{G}_3 \to 3$, $\mathcal{G}_4 \to 1$, $\mathcal{G}_5 \to 3$, $\mathcal{G}_6 \to 0$, $\mathcal{G}_8 \to 3$, $\mathcal{G}_9 \to 1$,, $\mathcal{G}_{10} \to 0$, $\mathcal{G}_{11} \to 1$, $\mathcal{G}_{12} \to 5$, $\mathcal{G}_{13} \to 2$, $\mathcal{G}_{14} \to 0$)
- Na posição correta, espera-se que apareçam 15% de 53 $\cong$ 8 caracteres "/" na mensagem (na verdade encontramos $\mathcal{G}_7 \to 11$).

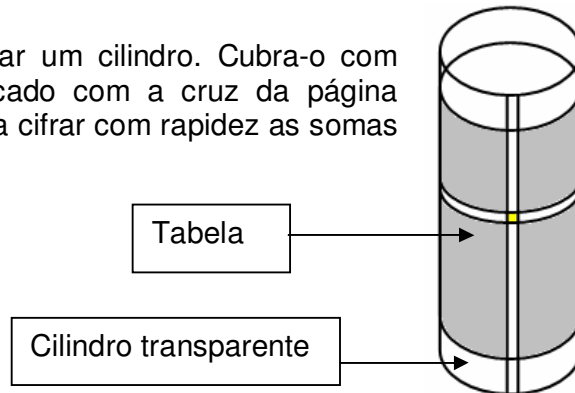
SIMULAÇÃO DA MÁQUINA DE LORENZ

Para confeccionar este aparato você vai precisar de um CD que não tenha mais uso e também de sua caixinha. Reproduza e recorte o círculo e cole-o no CD. O CD deve ser colocado dentro da caixinha.

Recorte o quadrado e coloque-o comodeve ser colocado na capa do CD. Para fazer a máquina funcionar você deve recortar na parte detrás da caixinha dois pequenos retângulos, suficientes para introduzir os dedos e girar o CD. Recorte as janelinhas indicadas nas setas.

Escolha as posições iniciais de $\mathcal{G}$ e $\mathcal{P}$
A Máquina de Lorenz
A letra codificada é obtida pela soma da letra original com as duas letras produzidas pela máquina
Engrenagem $\mathcal{P}$
Escolha a seguir um número entre 1 a 4 para a posição inicial de $\mathcal{P}$
Engrenagem $\mathcal{G}$
Escolha primeiramente um número entre 1 e 14 para a posição inicial de $\mathcal{G}$
Feche as janelas não utilizadas e gire na parte posterior

CILINDRO PARA SOMAS BINÁRIAS DA MÁQUINA DE LORENZ

Recorte e cole a aba para formar um cilindro. Cubra-o com outro cilindro transparente maior fabricado com a cruz da página seguinte. O aparato pode ser usado para cifrar com rapidez as somas binárias usadas na Máquina de Lorenz.

M Á Q U I N A 9 9 D E 9 9 L O R E N Z

ADIÇÃO DE LETRAS

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	9	8	+	4	3	/
A	/	G	F	R	4	C	B	Q	S	3	N	Z	8	K	+	Y	H	D	I	W	9	X	T	V	P	L	U	M	O	E	J	A
B	G	/	Q	T	O	H	A	F	8	L	P	J	S	Y	E	K	C	W	M	D	V	U	R	9	N	3	X	I	4	+	Z	B
C	F	Q	/	U	K	A	H	G	3	S	E	M	L	4	P	O	B	9	J	V	D	T	X	W	+	8	R	Z	Y	N	I	C
D	R	T	U	/	3	9	W	X	K	4	I	+	Y	S	Z	8	V	A	N	B	C	Q	G	H	M	O	F	P	L	J	E	D
E	4	O	K	3	/	N	+	Y	U	R	C	W	X	F	B	Q	P	J	9	Z	I	8	L	M	H	T	S	V	G	A	D	E
F	C	H	A	9	N	/	Q	B	J	I	4	8	Z	E	Y	+	G	U	3	X	R	W	V	T	O	M	D	L	P	K	S	F
G	B	A	H	W	+	Q	/	C	M	Z	Y	3	I	P	4	N	F	T	8	R	X	9	D	U	K	J	V	S	E	O	L	G
H	Q	F	G	X	Y	B	C	/	L	8	+	I	3	O	N	4	A	V	Z	9	W	R	U	D	E	S	T	J	K	P	M	H
I	S	8	3	K	U	J	M	L	/	F	D	H	G	R	V	T	Z	N	A	P	E	O	Y	+	W	Q	4	B	X	9	C	I
J	3	L	S	4	R	I	Z	8	F	/	9	B	Q	U	W	X	M	E	C	+	N	Y	O	P	V	G	K	H	T	D	A	J
K	N	P	E	I	C	4	Y	+	D	9	/	X	W	A	Q	B	O	S	R	8	3	Z	M	L	G	V	J	T	H	F	U	K
L	Z	J	M	+	W	8	3	I	H	B	X	/	C	V	R	9	S	O	Q	4	Y	N	E	K	U	A	P	F	D	T	G	L
M	8	S	L	Y	X	Z	I	3	G	Q	W	C	/	T	9	R	J	P	B	N	+	4	K	E	D	F	O	A	U	V	H	M
N	K	Y	4	S	F	E	P	O	R	U	A	V	T	/	H	G	+	I	D	M	J	L	8	Z	B	X	3	W	Q	C	9	N
O	+	E	P	Z	B	Y	4	N	V	W	Q	R	9	H	/	C	K	L	X	3	8	I	J	S	F	D	M	U	A	G	T	O
P	Y	K	O	8	Q	+	N	4	T	X	B	9	R	G	C	/	E	M	W	I	Z	3	S	J	A	U	L	D	F	H	V	P
Q	H	C	B	V	P	G	F	A	Z	M	O	S	J	+	K	E	/	X	L	U	T	D	9	R	4	I	W	3	N	Y	8	Q
R	D	W	9	A	J	U	T	V	N	E	S	O	P	I	L	M	X	/	K	G	F	H	B	Q	8	+	C	Y	Z	3	4	R
S	I	M	J	N	9	3	8	Z	A	C	R	Q	B	D	X	W	L	K	/	Y	4	+	P	O	T	H	E	G	V	U	F	S
T	W	D	V	B	Z	X	R	9	P	+	8	4	N	M	3	I	U	G	Y	/	Q	C	A	F	S	E	H	K	J	L	O	T
U	9	V	D	C	I	R	X	W	E	N	3	Y	+	J	8	Z	T	F	4	Q	/	B	H	G	L	P	A	O	M	S	K	U
V	X	U	T	Q	8	W	9	R	O	Y	Z	N	4	L	I	3	D	H	+	C	B	/	F	A	J	K	G	E	S	M	P	V
W	T	R	X	G	L	V	D	U	Y	O	M	E	K	8	J	S	9	B	P	A	H	F	/	C	I	4	Q	N	3	Z	+	W
X	V	9	W	H	M	T	U	D	+	P	L	K	E	Z	S	J	R	Q	O	F	G	A	C	/	3	N	B	4	I	8	Y	X
Y	P	N	+	M	H	O	K	E	W	V	G	U	D	B	F	A	4	8	T	S	L	J	I	3	/	9	Z	R	C	Q	X	Y
Z	L	3	8	O	T	M	J	S	Q	G	V	A	F	X	D	U	I	+	H	E	P	K	4	N	9	/	Y	C	R	W	B	Z
9	U	X	R	F	S	D	V	T	4	K	J	P	O	3	M	L	W	C	E	H	A	G	Q	B	Z	Y	/	+	8	I	N	9
8	M	I	Z	P	V	L	S	J	B	H	T	F	A	W	U	D	3	Y	G	K	O	E	N	4	R	C	+	/	9	X	Q	8
+	O	4	Y	L	G	P	E	K	X	T	H	D	U	Q	A	F	N	Z	V	J	M	S	3	I	C	R	8	9	/	B	W	+
4	E	+	N	J	A	K	O	P	9	D	F	T	V	C	G	H	Y	3	U	L	S	M	Z	8	Q	W	I	X	B	/	R	4
3	J	Z	I	E	D	S	L	M	C	A	U	G	H	9	T	V	8	4	F	O	K	P	+	Y	X	B	N	Q	W	R	/	3
/	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	9	8	+	4	3	/
	A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**9**	**8**	**+**	**4**	**3**	**/**

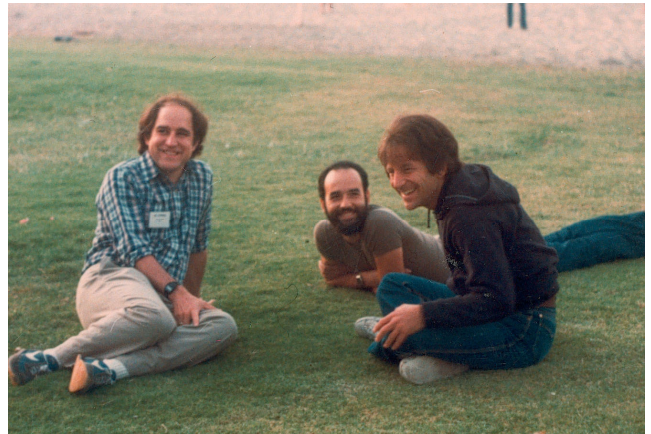
Estamos chegando ao fim de nossa viagem pela história da Criptologia. Nossa última parada será na atual época, em que os computadores desempenham um papel central na troca de mensagens sigilosas.

1977

Criptografia na era da Internet

Criptografia RSA para leigos

Os tradicionais meios de envio de mensagens secretas são baseados em chaves que devem ser distribuídas entre os participantes da comunicação. Nos tempos antigos, os espiões (hoje em dias os *hackers*), de posse destas chaves, podiam ameaçar o sigilo das mensagens, "quebrando o código". O problema de distribuição de chaves tornava assim frágeis muitos sistemas de comunicação sigilosa.

Por volta do ano de 1977 houve, entretanto, uma verdadeira mudança, diminuindo muito a fragilidade dos sistemas criptográficos. Tal façanha foi realizada por Ronald Rivest, Adi Shamir, and Leonard Adleman (foto), que elaboraram um sistema com duas chaves fortemente baseada em teoremas clássicos da Teoria dos Números. Este sistema, amplamente em uso, é chamado de RSA (iniciais dos sobrenomes dos três autores).

Uma das chaves serve para cifrar mensagens e pode ser divulgada livremente – todos têm acesso a ela – por isto mesmo é conhecida como chave pública. Por outro lado, para decifrar mensagens, há a necessidade de uma chave secreta, conhecida apenas pelo indivíduo para o qual a mensagem foi enviada, por isto esta chave é conhecida como chave secreta.

O método de criptografia RSA baseia-se neste sistema de chaves duplas e na impossibilidade prática de se obter a chave secreta a partir da chave pública. Isto se deve ao fato de não se conhecer atualmente algoritmos para decompor números grandes em fatores primos em um tempo razoável – uma impossibilidade tecnológica.

Nos sistemas de chave pública, cada pessoa possui um procedimento C para que os outros lhes enviem mensagens criptografadas. Estes procedimentos são conhecidos por todos – eles são publicados em uma lista (como a telefônica) ou estão disponíveis na Internet. Cada pessoa deve guardar secretamente um segundo procedimento D (sua senha secreta) para decifrar mensagens recebidas. O procedimento D desfaz ou inverte o procedimento C.

EXEMPLO DO FUNCIONAMENTO DO SISTEMA RSA

A idéia é transformar letras em números e construir uma função bijetora **C** definida no conjunto numérico obtido para usá-la na codificação de mensagens. A função inversa de **C** será denotada por **D** e usada para decifrar as mensagens criptografadas.

Qualquer função bijetora serve para este processo funcionar; entretanto se for fácil obter **D** a partir de **C**, será também fácil "quebrar o código", tornando o sistema frágil. O método RSA nos fornece uma maneira de se obter as funções **C** e **D** com bastante segurança.

Como implementar o RSA:

1) Escolha dois números primos distintos p e q e seja n = p.q.

Faremos a escolha p = 2 e q = 5 como um exemplo. Neste caso n = 2.5 = 10. Estaremos interessados em obter o resto da divisão de um dado número por n. Neste exemplo em que n = 10, o resto é sempre o algarismo das unidades do número, o que facilita muito o entendimento do método.

2) Escolha um número c que não tenha fatores comuns e que seja menor do que (p-1).(q-1).

No exemplo escolhido (p-1).(q-1) = 1.4 = 4 e **c** = 3 é a única opção.

3) Escolha um número d diferente de c tal que c.d – 1 seja múltiplo de (p-1).(q-1).

Seguindo o exemplo, vamos escolher **d** = 7. Este valor serve pois 3.7 – 1 = 20 = 5.4.

Pronto! Podemos construir nossas chaves para cifrar e decifrar mensagens:

Chave pública	Chave secreta
(n, **c**)	(n, **d**)
Ex: (10,3)	Ex: (10,7)

Como n =10, só conseguiremos trabalhar com números menores do que 10. Por isto vamos codificar apenas palavras cujas letras são as nove mais frequentes em português: A, E, O, S, R, I, N, D e M. Efetuamos primeiramente uma pré-codificação, trocando as letras por números:

A	E	O	S	R	I	N	D	M
1	2	3	4	5	6	7	8	9

Usaremos os números **c** e **d** escolhidos acima para fabricar funções bijetoras

$$\mathbf{C} : \{1,2,3,4,5,6,7,8,9\} \rightarrow \{1,2,3,4,5,6,7,8,9\}$$

$$n \mapsto \mathbf{C}(n)$$

$$\mathbf{D} : \{1,2,3,4,5,6,7,8,9\} \to \{1,2,3,4,5,6,7,8,9\}$$
$$n \mapsto \mathbf{D}(n)$$

tais que $\mathbf{C} \circ \mathbf{D} = \mathbf{D} \circ \mathbf{C} =$ Identidade.

A função **C**(n) é definida do seguinte modo: elevamos o número n à potência **c** e tomamos o resto da divisão por 10 do resultado obtido. A função **D**(n) é obtida de modo similar: elevamos o número n à potência **d** e tomamos o resto da divisão por 10 do resultado encontrado.

Vejamos um exemplo: vamos codificar a palavra ONDINA, usando as chaves do exemplo.

O-N-D-I-N-A torna-se, devido à pré-codificação, 3 – 7 – 8 – 6 – 7 – 1.

Usamos a chave pública **c** = 3 como potência e calculamos: 3^3 - 7^3 - 8^3 - 6^3- 7^3 - 1^3, o que dá 27 – 343 – 512 – 216 – 343 - 1. Tomamos o resto, na divisão por 10, de cada um destes números.. O resultado é 7 – 3 – 2 – 6 – 3 - 1. De fato a função **C** tem os seguintes valores:

n	1	2	3	4	5	6	7	8	9
n^3	1	8	27	64	125	216	343	512	729
C(n)= resto da divisão de n^3 por 10	1	8	7	4	5	6	3	2	9

Transformando agora números em letras, vemos que ONDINA fica codificada como NOEIOA.

Para decifrar, procedemos de modo análogo, usando a chave **d**:

Fazemos a pré-codificação de NOEIOA, obtendo 7 – 3 – 2 – 6 – 3 – 1 e elevamos cada um desses números à potência **d** = 7 : $7^7 – 3^7 – 2^7 – 6^7 – 3^7 – 1^7$. Finalmente tomamos o resto da divisão desses números por 10, ou seja, aplicamos a função de decodificação **D**(n).

n	1	2	3	4	5	6	7	8	9
n^7	1	128	2187	16384	78125	279936	823543	297152	4782969
D(n)= resto da divisão de n^7 por 10	1	8	7	4	5	6	3	2	9

O resultado, é claro, é 3 – 7 – 8 – 6 – 7 – 1, que quando trocado por letras recupera a palavra ONDINA.

Para entender porque o método acima funciona, leia o livro "Números inteiros e Criptografia RSA" de Severino Collier.

Será que podemos descobrir **d**, a partir de **c** e de **n**? No caso em que **n** é um número pequeno (no nosso exemplo **n** = 10), é fácil descobrir seus fatores primos (2 e 5). Assim (p-1).(q-1) é conhecido e não é muito difícil encontrar a chave secreta **d**, a partir da chave pública **c**. Entretanto, se p e q forem números muito grandes, a fatoração de **n** é muito demorada, praticamente impossível com nossa tecnologia atual. E, de fato, esta deficiência tecnológica é o que permite a utilização quase segura do sistema criptográfico RSA.

Para evitar que o código seja quebrado pela contagem das frequências das letras, pode-se agrupar as letras em blocos de diferentes tamanhos, antes de se iniciar o processo de codificação (depois disto os formatos dos blocos não podem mais ser alterados).

Para ilustrar nossos estudos, vamos apresentar agora algumas simulações simples com criptografia de chave pública.

SIMULAÇÕES COM CRIPTOGRAFIA DE CHAVE PÚBLICA

ENVIO DE MENSAGEM SIMPLES SEM ASSINATURA

Suponha que uma pessoa **A** deseje mandar uma mensagem secreta para outra pessoa **B**. Como cada pessoa tem duas chaves, uma pública e outra secreta, vamos denotar por $\mathbf{C_B}$ o procedimento usado para cifrar mensagens dirigidas a **B** e por $\mathbf{D_B}$ o procedimento que **B** usa para decifrar as mensagens que recebe.

Seja ***M*** a mensagem sem codificação alguma que **A** vai enviar a **B**. Para fazer isto, **A** codifica ***M*** e obtém $\mathbf{C_B}(M)$.

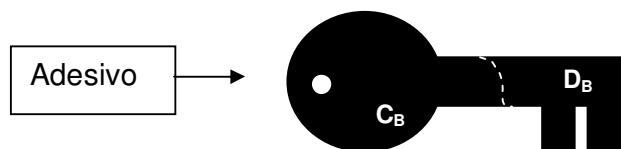
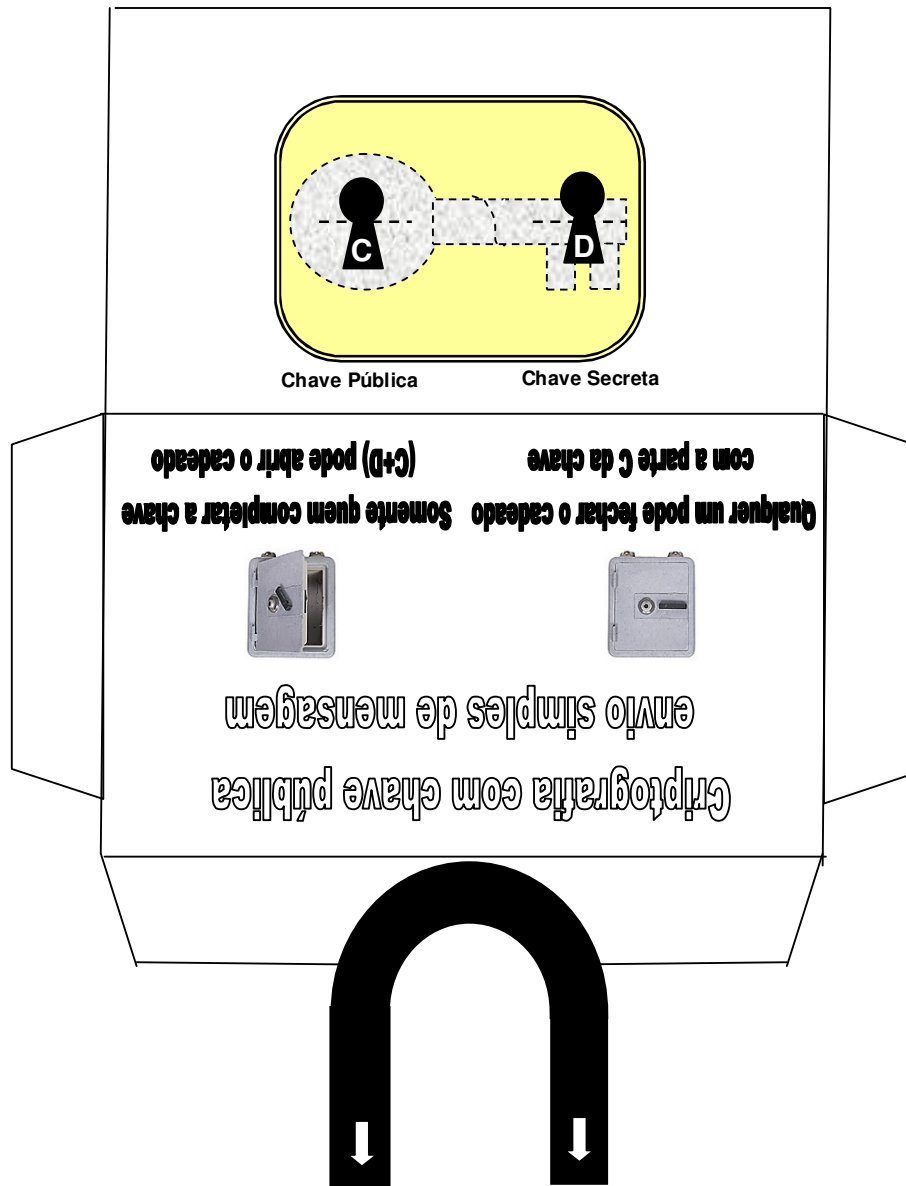
Quando **B** recebe a mensagem codificada, só ele pode decifrá-la, pois só ele conhece $\mathbf{D_B}$. Assim, realizando a operação

$$\mathbf{D_B (C_B (}M\mathbf{)) =} \; M$$

ele recupera ***M***, já que $\mathbf{D_B}$ desfaz a operação $\mathbf{C_B}$. Simples, não? Será que este sistema é seguro? Bem, é claro, isto depende das escolhas das chaves usadas.

ATIVIDADE

Nesta atividade você vai recortar e montar um envelope que será usado para receber em seu interior a mensagem ***M*** que **A** deseja enviar a **B**. Você deve recortar também os dois adesivos que farão o papel das chaves $\mathbf{C_B}$ e $\mathbf{D_B}$. Depois disto pronto,

a) Você fará o papel do emissor **A** e um amigo do receptor **B**. Segure o envelope com você, coloque a chave $\mathbf{C_B}$ (que é pública) em um espaço entre você e seu amigo e entregue para ele a chave $\mathbf{D_B}$ (que é secreta). Somente seu amigo tem a posse de $\mathbf{D_B}$, enquanto que qualquer um pode ter acesso a $\mathbf{C_B}$.
b) Escreva uma mensagem em um pedaço de papel e coloque-o dentro do envelope.
c) Proceda a **pré-codificação**, isto é, feche o cadeado, colocando as duas trancas nas fechaduras.
d) Levante a primeira dessas trancas e cole na fechadura correspondente o adesivo com a chave $\mathbf{C_B}$. Com isto você acabou de criptografar a mensagem.
e) Envie o envelope ao seu amigo.
f) Após recebê-lo, ele levanta a segunda tranca, cola sua chave secreta $\mathbf{D_B}$ e o envelope está aberto! A mensagem pode então ser lida com segurança.

ENVIO DE MENSAGENS ASSINADAS COM CHAVE PÚBLICA

Vimos que nos sistemas de chave pública, cada pessoa possui um procedimento **C** para que os outros lhes enviem mensagens criptografadas - estes procedimentos são conhecidos por todos pois estão publicados em uma lista (como se fosse o número de nossa conta-corrente em uma lista de um banco, ou uma lista telefônica) – e também um procedimento **D** que a pessoa deve guardar secretamente - sua senha secreta - para decifrar mensagens recebidas. Os procedimentos **C** e **D** anulam um o efeito do outro, ou seja as operações **C** e **D** comutam e as operações **C** seguida de **D** e **C** seguida de **D** são a identidade **I**(x) = x.

Suponha que uma pessoa **A**, tenha procedimentos $\mathbf{C_A}$ para cifrar mensagens e $\mathbf{D_A}$ para decifrar. Do mesmo modo, suponha que uma outra pessoa **B** possua procedimentos análogos $\mathbf{C_B}$ e $\mathbf{D_B}$. A pessoa **A** deseja mandar à pessoa **B** uma mensagem **M**. Ela faz isto enviando a seguinte mensagem codificada:

$$\mathbf{C_B(D_A)(M)}$$

Quando **B** recebe a mensagem codificada, só ele pode decifrá-la, pois só ele conhece $\mathbf{D_B}$. Assim, realizando a operação

$$\mathbf{D_B(C_B(D_A(M))) = D_A(M)}$$

ele obtém $\mathbf{D_A(M)}$. Observe que o processo para decifrar $\mathbf{D_A}$ exige a chave $\mathbf{C_A}$ que é pública! Deste modo ele consegue obter $\mathbf{C_A(D_A(M)) = M}$, ou seja, ele e só ele consegue ler a mensagem enviada por **A**.

A pessoa **B** tem certeza que foi **A** que lhe mandou a mensagem pois só ele poderia usar $\mathbf{D_A}$, isto é, só ele consegue calcular $\mathbf{D_A(M)}$ (a assinatura de **A** vem junto com a mensagem criptografada) e, em resumo, somente **B** consegue recuperar a mensagem pois só ele conhece $\mathbf{D_B}$ e ele tem certeza que foi a pessoa **A** que lhe mandou a mensagem pois só **A** conhece $\mathbf{D_A}$.

Veja como podemos simular esta situação toda usando envelopes:

ATIVIDADE

Nesta atividade você vai recortar e montar um envelope que será usado para receber em seu interior a mensagem ***M*** que **A** deseja enviar a **B**. Você deve recortar também os dois adesivos (chaves) $\mathbf{C_A}$, $\mathbf{D_A}$, $\mathbf{C_B}$ e $\mathbf{D_B}$. Depois disto pronto,

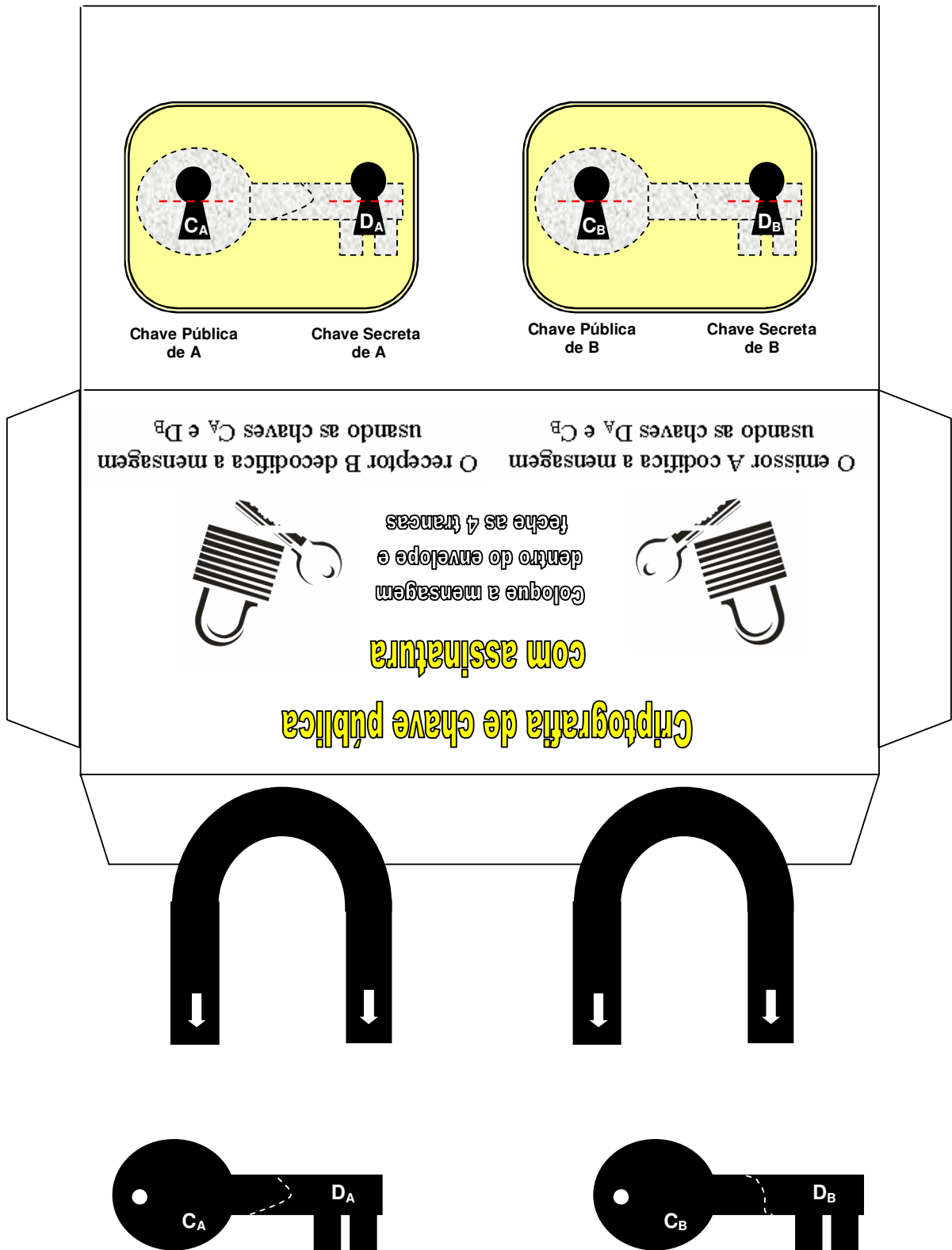
a) Você fará o papel do emissor **A** e um amigo do receptor **B**. Segure o envelope com você, coloque as chaves $\mathbf{C_A}$ e $\mathbf{C_B}$ (que são públicas) em um espaço sobre uma mesa entre você e seu amigo. Segure com você

sua chave secreta D_A e peça ao seu amigo que ele segure e mantenha em segredo sua chave secreta D_B .

Somente você tem a posse de D_A, enquanto que qualquer um pode ter acesso a C_A . Do mesmo modo, somente B conhece D_B, enquanto todos podem ter acesso a C_B.

b) Escreva uma mensagem **M** em um pedaço de papel e coloque-o dentro do envelope.
c) Proceda a **pré-codificação**, isto é, feche os cadeados, colocando as quatro trancas (duas de cada cadeado).
d) Levante a tranca correspondente ao adesivo D_A e cole este adeviso no local. No outro cadeado, abra a tranca C_B e cole no local o dadesivo correspondente. Isto completa a criptografia da mensagem, isto é você obteve com a chave primeira dessas trancas e cole na fechadura correspondente o adesivo com a chave C_B. Com isto você acabou de criptografar a mensagem. Você obteve $C_B(D_A(M))$.
e) Envie o envelope ao seu amigo.
f) Após recebê-lo, ele deve levantar a tranca do cadeado C_B e completar a chave, colando seu adesivo secreto D_B; a seguir deve levantar a tranca do cadeado com D_A, e colar o adesivo público C_A que estava sobre a mesa. Pronto! O envelope está aberto e a mensagem pode ser lida com segurança.

Somente **B** pode realizar esta sequência completa de decriptação (pois só ele tem a chave D_B) e o envelope prova que a mensagem veio certamente de **A,** pois a assinatura D_A ficou registrada nele.

CA
DA
CB
DB
Chave Pública de A
Chave Secreta de A
Chave Pública de B
Chave Secreta de B
O receptor B decodifica a mensagem usando as chaves CA e DB
O emissor A codifica a mensagem usando as chaves DA e CB
Coloque a mensagem dentro do envelope e feche as 4 trancas
Criptografia de chave pública com assinatura
CA
DA
CB
DB

JOGO DE BARALHO CODIFICADO

Veremos agora um sistema de criptografia que permite jogos (por exemplo de cartas) a distância que é bastante seguro, não permitindo trapaças (bom..., teoricamente, é claro!).

Vamos descrever um jogo com 52 cartas com dois jogadores. As cartas serão designadas por M_1, M_2, ..., M_{52}. Cada jogador deve escolher uma maneira de codificar (C) e outra maneira (D) de decifrar mensagens. Devemos escolher um procedimento bem elaborado, de modo que não possamos descobrir D a partir de C.

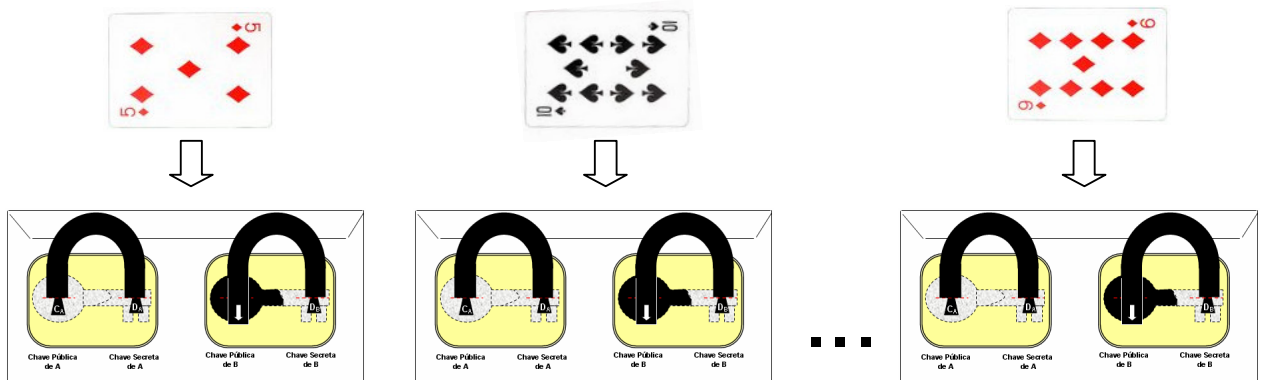
Jogador	Chave para codificar	Chave para decodificar
A	C_A	D_A
B	C_B	D_B

Seja M o valor de uma carta. Então $C_A(M)$ é o valor da carta M codificada pela chave pública de A. Podemos imaginar a carta M dentro de um envelope, como na atividade de criptografia de chave pública com assinatura. Como jogar?

1º.) O jogador A embaralha as cartas e as envia ao jogador B.

2º.) O jogador B codifica as 52 cartas do baralho obtendo

$C_B(M_1)$, $C_B(M_2)$, … , $C_B(M_{52})$

(Ele coloca as cartas em envelopes e utiliza a chave pública C_B)

O segundo jogador (B) embaralha os envelopes e envia-os ao primeiro jogador (A).

3º.) O jogador A escolhe 5 envelopes aleatoriamente e manda-os de volta ao jogador B. Estes envelopes contém as cartas que B utilizará no jogo. Digamos que dentro dos envelopes estão as cartas M_{i1}, M_{i2}, M_{i3}, M_{i4} e M_{i5}. O primeiro jogador (A) não sabe quais foram as 5 cartas escolhidas pois elas foram codificadas por B.

4º.) Recebendo os 5 envelopes vindos de A, o jogador B utiliza sua chave secreta D_B e descobre quais são suas cartas:

$M_{i1}= D_BC_B(M_{i1})$, $M_{i2}= D_BC_B(M_{i2})$, $M_{i3}= D_BC_B(M_{i3})$, $M_{i4}= D_BC_B(M_{i4})$, $M_{i5}= D_BC_B(M_{i5})$.

(Este procedimento é simulado pela colocação da chave D_B no lugar correspondente do envelope)

5º.) O primeiro jogador (A) seleciona agora suas cartas e as codifica com C_A: como as cartas já estavam anteriormente codificadas por B, o resultado obtido será:

$C_AC_B(M_{j1})$, $C_AC_B(M_{j2})$, $C_AC_B(M_{j3})$, $C_AC_B(M_{j4})$, $C_AC_B(M_{j5})$.

Neste ponto precisamos ter a garantia que uma propriedade fundamental das chaves seja válida: as chaves C_A e C_B devem comutar. Isto significa que as cartas codificadas acima são precisamente as cartas:

$C_BC_A(M_{j1})$, $C_BC_A(M_{j2})$, $C_BC_A(M_{j3})$, $C_BC_A(M_{j4})$, $C_BC_A(M_{j5})$.

6º.) O jogador A envia estas cartas duplamente codificadas (com 2 cadeados) ao jogador B que as decodifica com sua chave D_B. O resultado então é:

$C_A(M_{j1})$, $C_A(M_{j2})$, $C_A(M_{j3})$, $C_A(M_{j4})$, $C_A(M_{j5})$.

Observe que o jogador B não tem como conhecer as cartas do jogador A pois ainda elas estão codificadas com C_A e somente o jogador A tem a chave secreta D_A.

7º.) O jogador B envia estas 5 últimas cartas ao jogador A, que finalmente as decodifica usando a chave D_A, obtendo finalmente M_{j1}, M_{j2}, M_{j3}, M_{j4} e M_{j5}.

O jogo pode então ser iniciado. Quando isto acontece, nenhum dos jogadores conhece as cartas do outro nem as cartas restantes. Note que as cartas do “morto” estão em poder do jogador A, mas codificadas com o cadeado C_B e a chave D_B encontra-se em poder do jogador B. Assim A não tem como decodificá-las. No fim do jogo, os jogadores podem revelar suas chaves e verificar se houve ou não trapaça!

CÓDIGO GENÉTICO

Mensagens secretas codificadas com DNA

Tinta com DNA impede falsificação

A falsificação de assinaturas, cheques, testamentos, obras de arte e outros documentos pode deixar de preocupar a polícia após a comercialização de uma tinta especial elaborada por dois argentinos. O médico legista Rubén Simonetta, um dos inventores, disse ao jornal La Nación que o produto é uma tinta invisível e inalterável, com moléculas encapsuladas do DNA da pessoa que vai utilizá-la, que deve ser aplicada sobre qualquer papel ou elemento suscetível de ser adulterado. As moléculas de DNA, que determinam características hereditárias como a cor dos olhos e do cabelo, constituem uma espécie de impressão digital, pessoal e única.

Você se lembra de antigamente quando um fio de bigode valia mais do que uma assinatura em um documento? Bom, se for possível extrair o DNA do fio de bigode, isto, de fato, é verdade.

O uso do DNA para codificar mensagens

Hoje em dia, com a engenharia genética, é possível codificar mensagens em uma porção de DNA que fique camuflada entre uma quantidade enorme de moléculas similares e que possam ser agrupadas em um espaço muito pequeno (menor do que um ponto final em uma carta, por exemplo). Isto foi apresentado primeiramente por Viviana Risca de Nova Iorque, no ano de 2000.

Uma porção de DNA é uma cadeia de moléculas denotadas pelas letras A, C, G e T, que são as iniciais de adenina, citosina, guanina e timina respectivamente. Essas bases ligam-se aos pares: as únicas ligações possíveis são AT, TA, CG e GC. O formato da dupla hélice do DNA deve-se à ligação de uma cadeia de bases com sua base complementar. Por exemplo a seqüência TAGCCT tem como seqüência complementar ATCGGA. Uma seqüência de três bases é chama de códon. Podemos usar os códons para cifrar mensagens, de acordo, por exemplo, com a tabela:

Chaves criptográficas e DNA			
A→ CGA	K → AAG	U → CTG	0 → ACT
B → CCA	L → TGC	V → CCT	1 → ACC
C → GTT	M → TCC	W → CCG	2 → TAG
D → TTG	N → TCT	X → CTA	3 → GAC
E → GGC	O → GGA	Y → AAA	4 → GAG
F → GGT	P → GTG	Z → CTT	5 → AGA
G → TTT	Q → AAC	- → ATA	6 → TTA
H → CGC	R → TCA	, → TCG	7 → ACG
I → ATG	S → ACG	. → GAT	8 → AGG
J → AGT	T → TTC	: → GCT	9 → GCG

Por exemplo, a mensagem “PERIGO À VISTA”, pode ser criptografada como GTG GGC TCA ATG TTT GGA CGA CCT ATG ACG TTC CGA. Esta seqüência de bases é colocada entre duas porções de DNA com 20 bases cada. Estas 20 bases são conhecidas apenas por quem envia e por quem recebe a mensagem. A codificação da mensagem “PERIGO À VISTA” tem 12 x 3 = 36 letras, que correspondem a 36 x 3 = 108 bases e que colocadas entre 20 bases iniciais e 20 bases finais perfazem 148 letras do código genético.

Por exemplo, a mensagem acima pode ser criptografada usando inicialmente TCCCTCTTCGTCGAGTAGCA, a própria mensagem GTGGGCTCAATGTTTGGACGACCTATGACGTTCCGA e o complemento de TCTCATGTACGGCCGTGAAT. Depois disto mistura-se algumas dessas moléculas com fragmentos de mesmo tamanho de DNA.

Somente quem conhece as 20 bases iniciais e as 20 bases finais será capaz de extrair a mensagem, usando-se uma técnica conhecida com reação de polimerase em cadeia, isolando assim o trecho de DNA que contém a mensagem a ser decifrada. Quem não conhece as bases iniciais e finais ficará com a tarefa de analisar 4^{20} possibilidades de sequências iniciais para encontrar o par correto de chaves. Desta maneira, pode-se enviar mensagens secretas, com segurança alta, em um espaço de dimensões ínfimas.

TROCA DE BEBÊS

Três bebês nasceram ao mesmo tempo na maternidade e, por descuido, ninguém se lembrou de colocar as identificações neles. E agora, você pode descobrir quem é filho de quem? Abaixo está o resultado de um teste que é feito com o DNA de cada um dos pais e dos bebês. A dica é que o bebê tem metade do DNA do pai e metade do DNA da mãe. Veja se consegue resolver a charada com base na posição dos tracinhos dos pais e dos filhos.

CASAL A		CASAL B		CASAL C		BEBÊ 1	BEBÊ 2	BEBÊ 3
João	Maria	Pedro	Ana	José	Rosa			
			■	■		■		■
■							■	
				■		■		
	■		■	■	■	■	■	
		■						■
	■		■					
	■						■	
■				■				
■		■			■			■
					■	■		
■		■					■	
			■					■
	■	■			■	■		

TEMAS DE BIOLOGIA

PROPOSTAS PARA DESENVOLVER EM SALA DE AULA

NÚMERO 1 JULHO DE 1995 EDITORA MODERNA

IDENTIFICANDO PESSOAS PELO DNA: UMA SIMULAÇÃO

J. M. Amabis* e G. R. Martho

Em maio de 1995, nos Estados Unidos, os promotores do julgamento de O. J. Simpson, ex-astro do futebol americano acusado de assassinar a esposa, pediram à bioquímica Robin Cotton que desse aos jurados uma aula sobre DNA, o material hereditário dos seres vivos. A análise do sangue encontrado no local do crime havia revelado a presença de DNA supostamente pertencente a Simpson.

O exemplo acima ilustra como conhecimentos antes restritos aos especialistas tornam-se hoje acessíveis ao grande público. As pessoas querem saber o que é DNA e por que ele é comparável a uma impressão digital que identifica seu portador.

Desenvolver e aproveitar temas como esse pode tornar mais interessante e produtivo o trabalho do professor em sala de aula. Neste número apresentamos uma proposta de atividade cujo principal objetivo é levar os estudantes a compreender a importância prática da Engenharia Genética na identificação de pessoas.

1ª. identificação foi na Inglaterra

O primeiro caso de identificação criminal através de exames de DNA ocorreu em 1985, na Inglaterra. Em um pequeno conda- do, rodeado de montanhas e com uma única estrada de acesso, uma mulher foi estuprada e assassinada.

"Lá havia um geneticista, Alec Jeffreys, que colheu o esperma encontrado na vítima e fez o exame de DNA. Mais tarde houve outro crime similar. Novamente Jeffreys analisou o sêmen encontrado na vítima. Era do mesmo homem que cometera o primeiro crime", conta José Maria Marlet, professor de medicina legal da USP.

As autoridades locais forjaram uma campanha de doação de sangue cuja finalidade era identificar o agressor. Todos os habit- antes foram doar sangue, mas nenhum deles possuía DNA igual ao do estuprador.

"A polícia prosseguiu com as investigações e descobriu que havia um viajante no condado. Quando o sujeito voltou, foi convidado a doar sangue. Feito o teste de DNA no sangue col- hido, Jeffreys concluiu que o código genético do viajante era o mesmo do estuprador", conta Marlet.

Fonte: Folha de São Paulo 28/05/95

As técnicas da Engenharia Genética permitem identificar pessoas pela análise de suas moléculas de DNA (ácido desoxirribonucléico), a substância que constitui os genes. Com exceção dos gêmeos univitelinos, cada pessoa possui um conjunto de genes, e portanto de moléculas de DNA, único e particular.

O processo mais simples para caracterizar um DNA consiste em cortar as moléculas dessa substância com o auxílio de "tesouras moleculares", as chamadas **enzimas de restrição**, analisando em seguida o tamanho dos fragmentos que se formaram. Uma enzima de restrição corta a molécula de DNA em pontos específicos, somente onde ocorre determinada seqüência de bases nitrogenadas. Como cada pessoa tem seqüências típicas de bases nitrogenadas, o número e os tamanhos dos fragmentos obtidos pelo corte enzimático acaba por caracterizar seu DNA.

O tamanho dos "fragmentos de restrição", como são chamados os fragmentos obtidos após o corte enzimático, é determinado através da técnica de **eletroforese**. A mistura de fragmentos de DNA é aplicada em uma camada de gelatina (gel) e submetida a um campo elétrico. Nessas condições, os fragmentos se movem a velocidades inversamente proporcionais ao seu tamanho, isto é, os fragmentos menores deslocam-se mais rapidamente que os maiores.

Quando o campo elétrico é desligado, fragmentos de mesmo tamanho estacionam juntos em determinada posição do gel, formando uma faixa. O padrão de faixas que surge é característico para cada pessoa, e corresponde à sua "impressão digital" genética.

Neste número sugerimos a simulação de experimentos nos quais amostras de DNA de diferentes pessoas são tratadas com uma enzima de restrição hipotética, que corta as moléculas onde houver dois pares de bases C-G/C-G em seqüência.

O preenchimento dos gráficos, onde os fragmentos do DNA cortado são dispostos por ordem de tamanho, simula a separação eletroforética.

Apresentamos, ainda, um processo simples e prático para extrair DNA de uma amostra, no caso, de células de cebola.

P. PLAILLY/SPL-STOCK PHOTOS

Foto de um gel de eletroforese iluminado com luz ultravioleta. Sob essa luz, o DNA previamente tratado fluoresce, revelando um padrão de faixas típico do DNA analisado.

* Professor do Departamento de Biologia do Instituto de Biociências da Universidade de São Paulo

Sugestões e pré-requisitos

Na página à direita apresentamos um modelo para a folha de atividades dirigida ao estudante. Nela se encontram todas as informações objetivas para resolver às duas questões formuladas: "Quem é o criminoso? Quem é o pai da criança?". As respostas a essas questões encontram-se no verso da folha de atividades.

Sugerimos que o professor oriente verbalmente o estudante sobre a diferença de procedimentos entre a detecção do criminoso e a do pai da criança. No primeiro caso basta encontrar, entre os suspeitos, um padrão eletroforético idêntico ao da amostra de pele sob as unhas da vítima. Já no segundo caso é preciso, inicialmente, identificar na criança as faixas eletroforéticas correspondentes à mãe, para em seguida procurar, nos pretendentes a pai, aquele que possui as faixas que faltam. Essas faixas devem estar necessariamente presentes no pai, uma vez que a criança recebe um cromossomo materno e um homólogo paterno.

No quadro abaixo fornecemos informações práticas para executar, na própria sala de aula, um experimento simples de extração de DNA. Apesar de simplificados, os procedimentos são muito parecidos aos utilizados nos laboratórios bioquímicos, e permitem ao estudante visualizar, ainda que macroscopicamente, o aspecto do material hereditário.

O tema será mais bem aproveitado se o estudante já dominar os conceitos básicos relativos às estruturas do DNA e dos cromossomos. Em nossas obras de Biologia esses assuntos podem ser encontrados nos seguintes volumes:

AMABIS, J. M. & MARTHO, G. R. *Fundamentos da Biologia moderna*, São Paulo, Ed. Moderna, 1997:
- Estrutura dos ácidos nucléicos (págs. 102-103);
- Genes: estrutura química e duplicação (págs. 152-153);
- Engenharia genética (págs. 540-545).

—— *Biologia das células* (vol. 1), São Paulo, Ed. Moderna, 1994:
- A estrutura dos cromossomos (págs. 178-180);
- Cromossomos e genes (págs. 182-185);
- A estrutura do gene (págs. 311-313).

—— *Biologia das populações* (vol. 3), São Paulo, Ed. Moderna, 1995:
- A base celular da hereditariedade (págs. 7-9).

Extraindo DNA em sala de aula

Material

- ✓ uma cebola grande (± 200 g)
- ✓ faca de cozinha
- ✓ dois copos tipo americano
- ✓ banho-maria (± 60 °C)
- ✓ água filtrada
- ✓ sal de cozinha
- ✓ detergente para louças
- ✓ álcool etílico 95% gelado (a cerca de –10 °C)
- ✓ bastão fino de vidro ou madeira
- ✓ coador de café, de papel
- ✓ gelo moído

Informações técnicas

A extração de DNA de células eucariontes consta fundamentalmente de três etapas: a) ruptura das células para liberação dos núcleos; b) desmembramento dos cromossomos em seus componentes básicos, DNA e proteínas; c) separação do DNA dos demais componentes celulares.

O bulbo de cebola foi usado por apresentar células grandes, que se rompem facilmente quando a cebola é picada.

O detergente desintegra os núcleos e os cromossomos das células da cebola, liberando o DNA. Um dos componentes do detergente, o dodecil (ou lauril) sulfato de sódio, desnatura as proteínas, separando-as do DNA cromossômico.

O álcool gelado, em ambiente salino, faz com que as moléculas de DNA se aglutinem, formando uma massa filamentosa e esbranquiçada.

Procedimentos

1. Pique a cebola em pedaços de 0,5 cm.
2. Coloque quatro colheres de sopa de detergente e uma colher das de chá de sal em meio copo d'água, mexendo bem até dissolver completamente.
3. Coloque a cebola picada no copo com a solução de detergente e sal, e leve ao banho-maria por cerca de 15 minutos.
4. Retire a mistura do banho-maria e resfrie-a rapidamente, colocando o copo no gelo durante cerca de 5 minutos.
5. Coe a mistura no coador de café, recolhendo o filtrado em um copo limpo.
6. Adicione ao filtrado cerca de meio copo de álcool gelado, deixando-o escorrer vagarosamente pela borda. Formam-se duas fases, a superior, alcoólica, e a inferior, aquosa.
7. Mergulhe o bastão no copo e, com movimentos circulares, misture as fases. Formam-se fios esbranquiçados, que são aglomerados de moléculas de DNA.

Técnica modificada de J. Schollar e D. Madden — Centro de Educação Biotecnológica da Universidade de Reading — Inglaterra

ATIVIDADE: IDENTIFICANDO PESSOAS PELO DNA

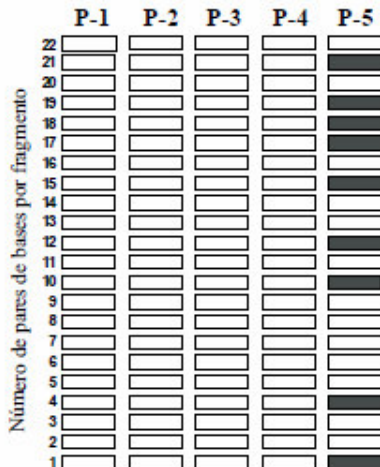
Nome: ______________________________ Série: ____________

Nesta atividade você aplicará os princípios da identificação de pessoas pelo DNA na solução de duas questões judiciais. Em uma delas identificará um criminoso entre três suspeitos, e em outra descobrirá quem é o pai de uma criança.

Ao lado estão representados segmentos de DNA de cinco pessoas (P-1 a P-5). Cada uma tem dois segmentos, correspondentes a um par de cromossomos homólogos (CA e CB). As seqüências de bases dos homólogos podem ser ligeiramente diferentes em função da diferença entre os genes alelos.

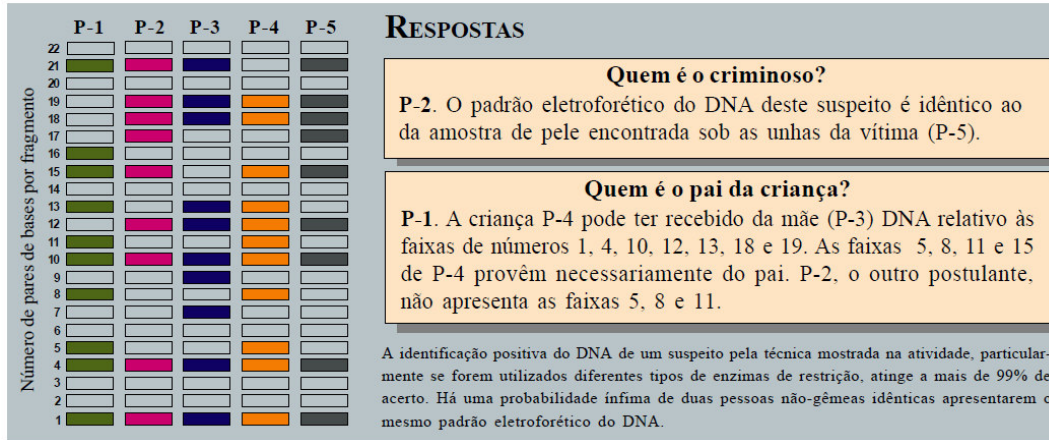
O primeiro passo para a análise do DNA é cortá-lo com uma enzima de restrição hipotética que, neste exemplo, reconhece a seqüência de dois pares de bases *C-G* adjacentes (dois *C* em uma cadeia e dois *G* na outra). Para facilitar, essas "seqüências de corte" estão destacadas no DNA. Localize, nos dois segmentos de DNA de cada pessoa, todas as seqüências de corte. Marque-as à lápis com um traço horizontal, de modo a separar um par *C-G* do par *C-G* adjacente.

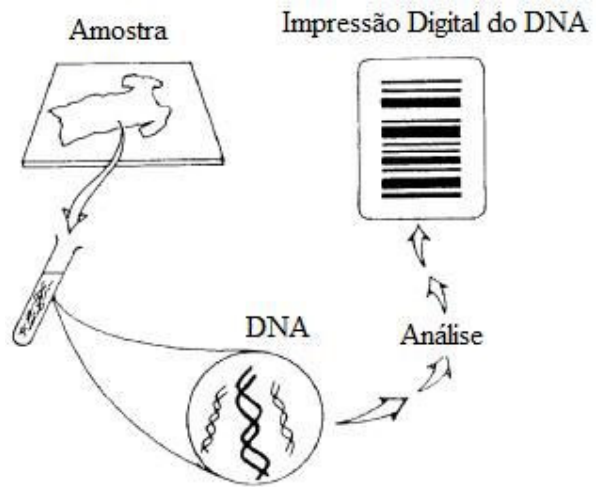
O passo seguinte é organizar os fragmentos obtidos por ordem de tamanho. Para isso, conte o número de pares de bases de cada fragmento e complete o preenchimento do gráfico localizado na parte inferior esquerda da figura. Cada coluna do gráfico simula o padrão eletroforético de uma pessoa, onde os fragmentos de DNA se distribuem em faixas por ordem de tamanho. A título de exemplo, a coluna correspondente ao padrão da pessoa P-5 já está preenchida.

A seguir, responda às questões abaixo.

Quem é o criminoso?

Restos de pele encontrados sob as unhas de uma pessoa assassinada foram submetidos ao teste de DNA, revelando o padrão eletroforético P-5. Três pessoas, P-1, P-2 e P-3, suspeitas do crime, também foram submetidas ao teste de DNA. Qual delas é a provável culpada?

Quem é o pai da criança?

Dois homens, P-1 e P-2, disputam a paternidade de uma criança, P-4, filha da mulher P-3. Com base no teste de DNA dos quatro implicados, quem é o provável pai da criança?

Impressão Digital Genética

A Impressão digital genética foi desenvolvida pelo professor Alan Jeffreys na Universidade de Leicester, em 1984. A técnica é baseada no fato de que cada indivíduo tem uma única composição genética, contida na molécula de DNA (ácido desoxirribonucléico), que é herdado dos pais biológicos, sendo metade da mãe e metade do pai. O DNA pode ser extraído de células, é coletado de materiais orgânicos e, após processado, produz um padrão de bandas ou a "impressão digital" do DNA.

Os testes de DNA têm sido usados em criminalística para resolver casos de homicídios, assaltos ou atentados; as secreções corporais encontradas na cena do crime podem ser comparadas às de um suspeito. É comum a comparação entre 10 e 20 bandas. Experimentos têm demonstrado que nas pessoas relatadas a probabilidade de uma banda coincidir é de uma em quatro, ou seja, a probabilidade é de ¼ (estimada usando-se a Lei dos Grandes Números).

Assim, por exemplo, a probabilidade de duas bandas coincidirem é igual a $(1/4)^2 = 1/16$. Ou seja, uma chance em dezesseis. Já probabilidade de 10 bandas coincidirem é de $(1/4)^{10} = 1/1048576$, aproximadamente uma chance em 1 milhão.

Se admitirmos, entretanto, que a probabilidade de coincidência de uma única banda ser de 0,5, para a coincidência de 10 bandas teremos $(1/2)^{10} = 1/1024$, aproximadamente uma chance em mil. Esta discrepância pode

dar origem a disputas judiciais; por isto um número maior de bandas devem ser comparadas.

ATIVIDADE: a) A população do Brasil é de cerca de 200 milhões de habitantes. Supondo que p = 0,25, qual o número de bandas que precisam ser comparadas para se obter probabilisticamente uma chance em 200 milhões de se encontrar pessoas com essas bandas coincidentes?

b) A população mundial está estimada em 6,4 bilhões de pessoas. Com p = 0,25, qual o número de bandas que precisam ser comparadas neste caso?

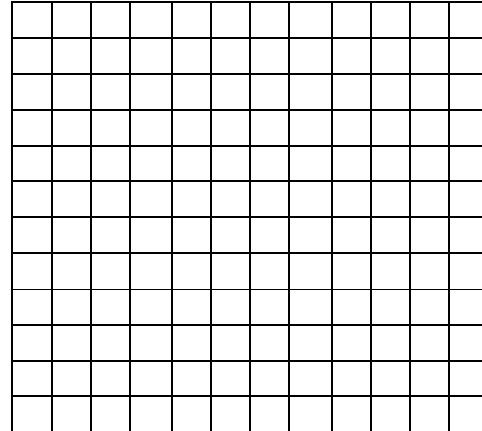
Mais geralmente, se p denota a probabilidade de coincidência de uma única banda em uma população com H habitantes, o número n de bandas que devem ser comparadas para se ter uma chance de coincidência no universo de H pessoas pode ser encontrado utilizando o logaritmo: $p^n = 1/H \rightarrow \log(p^n) = \log(1/H) \rightarrow n \log p = -\log H \rightarrow n = -(\log H)/\log p$.

ANTICRIPTOGRAFIA: COMUNICAÇÃO COM EXTRA-TERRESTRES

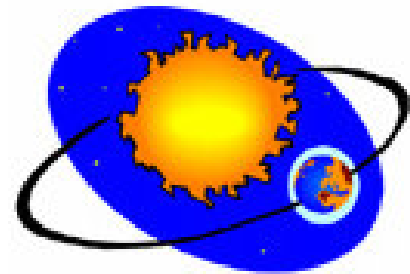
Todas as atividades feitas até agora tinham o objetivo de ocultar, de algum modo, as informações de uma mensagem. Mas existe também o problema inverso: como fazer para que uma mensagem seja entendida de modo fácil por alguém que não fala nossa língua e não está acostumado com nossos códigos de escrita?

Admitindo-se a possibilidade de vida em outros planetas, quais seriam as maneiras mais simples de estabelecer comunicação com estes seres? Muita gente já pensou nisto, acredite. Uma primeira sugestão seria construir um enorme painel luminoso que pudesse ser visto do espaço, provavelmente com alguma informação geométrica (círculos, quadrados, algum teorema sobre triângulos, talvez). Uma outra sugestão estaria baseada na Aritmética, na conhecida sequência dos números naturais: 1, 2, 3, ...; se algum sinal puder ser capturado por algum alienígena, esta sequência poderia ser enviada como bip, bip-bip, bip-bip-bip,...Talvez alguma operação aritmética elementar também pudesse ser enviada: bip-bip (tempo) bip-bip (tempo) bip-bip-bip-bip.

Com uma sequência de 0 e 1, podemos formar píxeis e transmitir mensagens e imagens (como é feito nos monitores de vídeo). Por exemplo, qual será a mensagem formada pela sequência abaixo?

111011101000
100010101000
111010101000
001010101000
111011101110
000000000000
100010101110
100010101010
100010101110
100010101010
111011101010
000000000000

(*pinte as respectivas casas marcadas com 1 na grade*)

Uma outra estranha maneira de se comunicar com extra-terrestres que tem interesse matemático é a apresentada por Martin Gardner em seu 6th Book of Mathematical Diversions from Scientific American, a qual descrevemos a seguir. A mensagem usa símbolos usuais do alfabeto, mas outros símbolos poderiam ser usados, sem problemas.

1. A. B. C. D. E. F. G. H. I. J. K. L. M. N. P. Q. R. S. T. U. V. W. Y. Z.
2. A A, B; A A A, C; A A A A, D; A A A A A, E; A A A A A A, F; A A A A A A A, G; A A A A A A A A, H; A A A A A A A A A, I; A A A A A A A A A A, J.
3. A K A L B; A K A K A L C; A K A K A K A L D. A K A L B; B K A L C; C K A L D; D K A L E. B K E L G; G L E K B. F K D L J; J L F K D.
4. C M A L B; D M A L C; I M G L B.
5. C K N L C; H K N L H. D M D L N; E M E L N.
6. J L AN; J K A L AA; J K B L AB; AA K A L AB. J K J L BN; J K J K J L CN. FN K G L FG.
7. B P C L F; E P B L J; F P J L FN.
8. F Q B L C; J Q B L E; FN Q F L J.
9. C R B L I; B R E L CB.
10. J P J L J R B L S L ANN; J P J P J L J R C L T L ANNN. J P S L T; J P T L J R D.
11. A Q J L U; U Q J L A Q S L V.
12. U L WA; U P B L WB; AWD M A L WD L D P U. V L WNA; V P C L WNC. V Q J L WNNA; V Q S L WNNNA. J P EWFGH L EFWGH; S P EWFGH L EFGWH.
13. GIWIH Y HN; T K C Y T. Z Y CWADAF.
14. D P Z P WNNIB R C Q C.

Não é difícil de descobrir o significado das coisas. Na linha 1 simplesmente estão declarados os símbolos que serão usados. Na linha 2 os 10 primeiros símbolos são identificados com os números de 1 a 10. Na linha 3 os símbolos de + e = são introduzidos. Na linha 4 o sinal de subtração – é introduzido e na linha 5 aparece o símbolo zero. A notação posicional é apresentada na linha 6. Observe que J = NA. A seguir, na linha 7 aparece o

sinal de multiplicação e na linha 8 o sinal de divisão. Na linha 9 estão definidos os expoentes. Os números 100 e 1000 aparecem na linha 10 e 1/10 e 1/100 na linha 11. Na linha 12 a vírgula usada na notação decimal é introduzida e o sinal de "aproximadamente igual" ≈ aparece na linha 13, bem como o valor aproximado de Pi: π ≈ 3,1416. Finalmente a linha 14 nos dá a expressão:

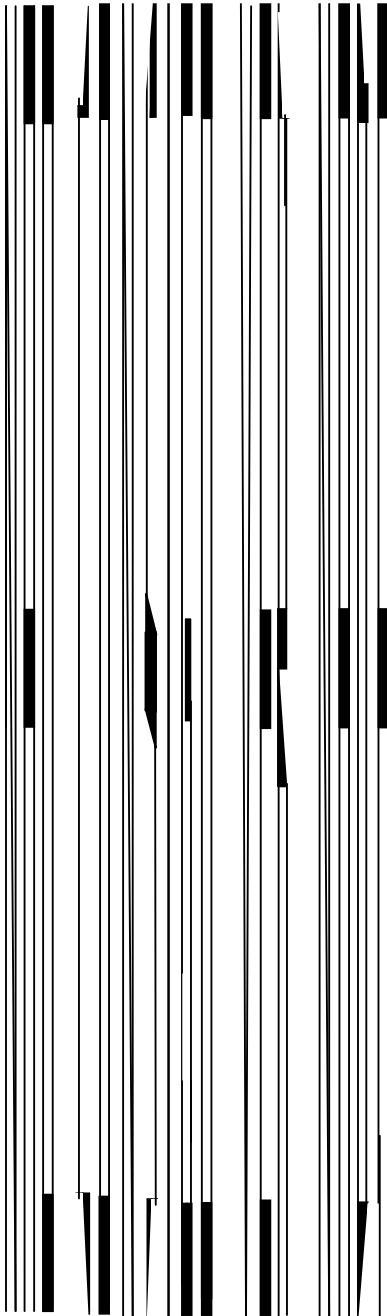
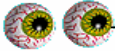
$$(4 \times \pi \times 0{,}0092^3) / 3$$

(desde que interpretemos as prioridades dos símbolos de uma determinada forma).

Que sentido tem esta última sentença? É claro que ela sugere o volume de uma esfera. Mas porque o raio 0,0092? Bem, se alguém do espaço exterior receber esta mensagem e localizar o sistema solar, tomando o raio do Sol como unidade, descobrirá que o raio do terceiro planeta mais distante desta estrela tem como medida de seu raio aproximadamente 0,0092 do raio do Sol. Acredita-se, desta forma que ele conseguirá localizar o planeta Terra. Incrível, não?

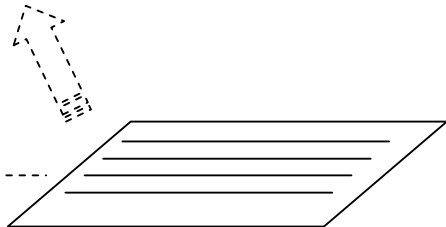
Veja, a seguir, o significado dos símbolos usados na mensagem (as letras O e X não são usadas):

A	B	C	D	E	F	G	H	I	J	K	L	M	N	P	Q	R	S	T	U	V	W	Y	Z
1	2	3	4	5	6	7	8	9	10	+	=	-	0	x	÷	eleva do a	100	1000	1/10	1/100	,	≈	π

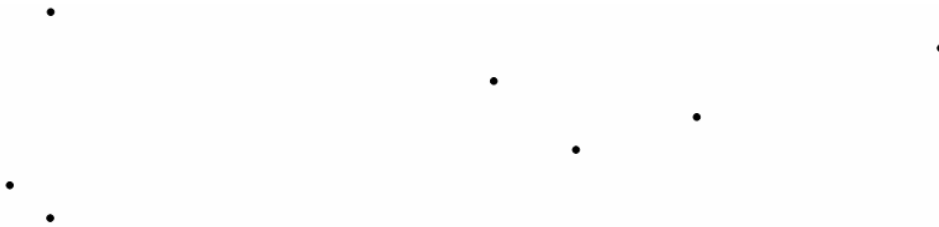
MÉTODOS ANTIGOS QUE OS ALUNOS USAVAM PARA COLAR

Querido professor, gostaríamos de parabenizá-lo pela bo-
a resposta do problema da avaliação fi-
nalizada este semestre na Escola. A escolha profissio-
nal é a primeira alternativa e somente o bo-
nito gesto realizado pelo senhor permanecerá em nossa memória. A tri-
bo do professor ainda não percebeu nos-
sa enorme gratidão pelo seu grandio-
so método de comunicação."

(leia mais uma vez, a partir da segunda linha, pulando alternadamente uma linha)

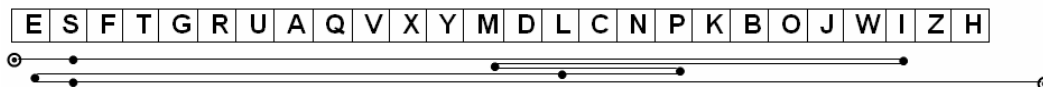
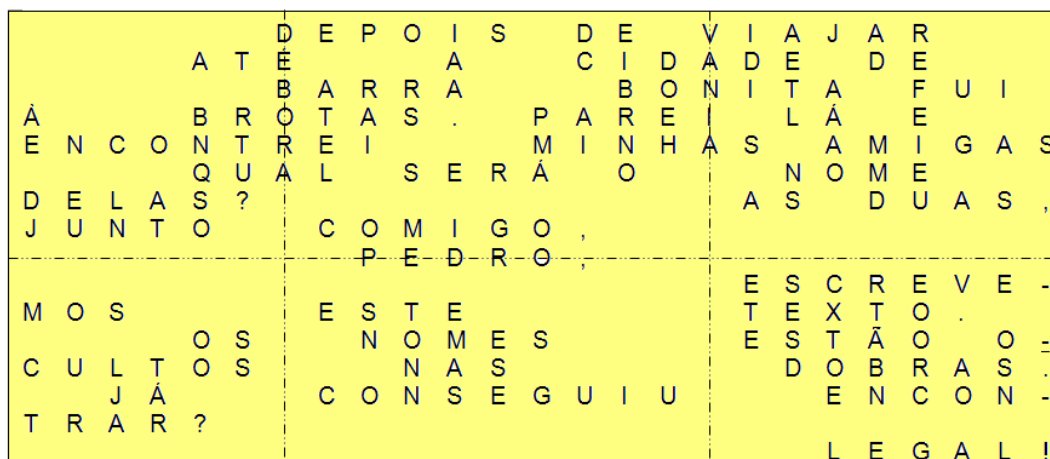
ZERO VIRADO.
vai tirar um
para cima, você
tudo de baixo
cola é escrever
fácil de passar
Uma maneira

(Anamorfose)

MENSAGEM SECRETA USANDO-SE PALAVRAS CRUZADAS

CÓDIGO DE PONTOS

O que significa a mensagem abaixo?

Use a grade para descobrir:

E	S	F	T	G	R	U	A	Q	V	X	Y	M	D	L	C	N	P	K	B	O	J	W	I	Z	H
	.																								
																							.		
												.													
																	.								
														.											
.																									
	.																								

Simples, não é? Como variação use um barbante bem comprido, dando nós nos pontos:

MÉTODO DA COLA NA DOBRA

MÉTODO DA DOBRA COM SIMETRIA:

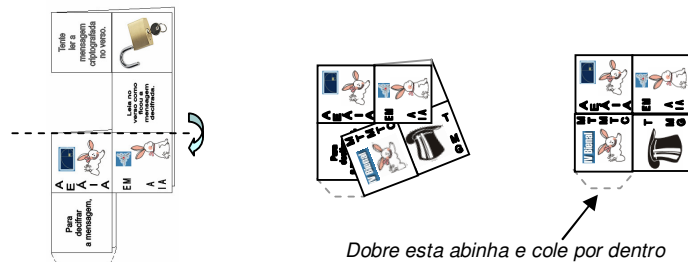
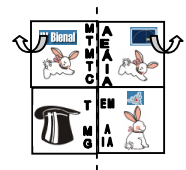
(dobre ao meio e leia contra a luz)

MÉTODO GIRATÓRIO

Os símbolos de rotação indicam os giros a partir da posição usual da folha.Que confuso!

CADEADO DE PAPEL

1. Copie e recorte a figura acima.

2. Dobre, como nas ilustrações

3. Gire o cadeado de 90º, ele está quase pronto e deve ter o formato:

4. Dobre-o pela linha pontilhada para trás e, após dobrar, abra ao meio como se fosse um livro. O resultado será o seguinte (cadeado mágico fechado). A mensagem no verso ficou embaralhada.

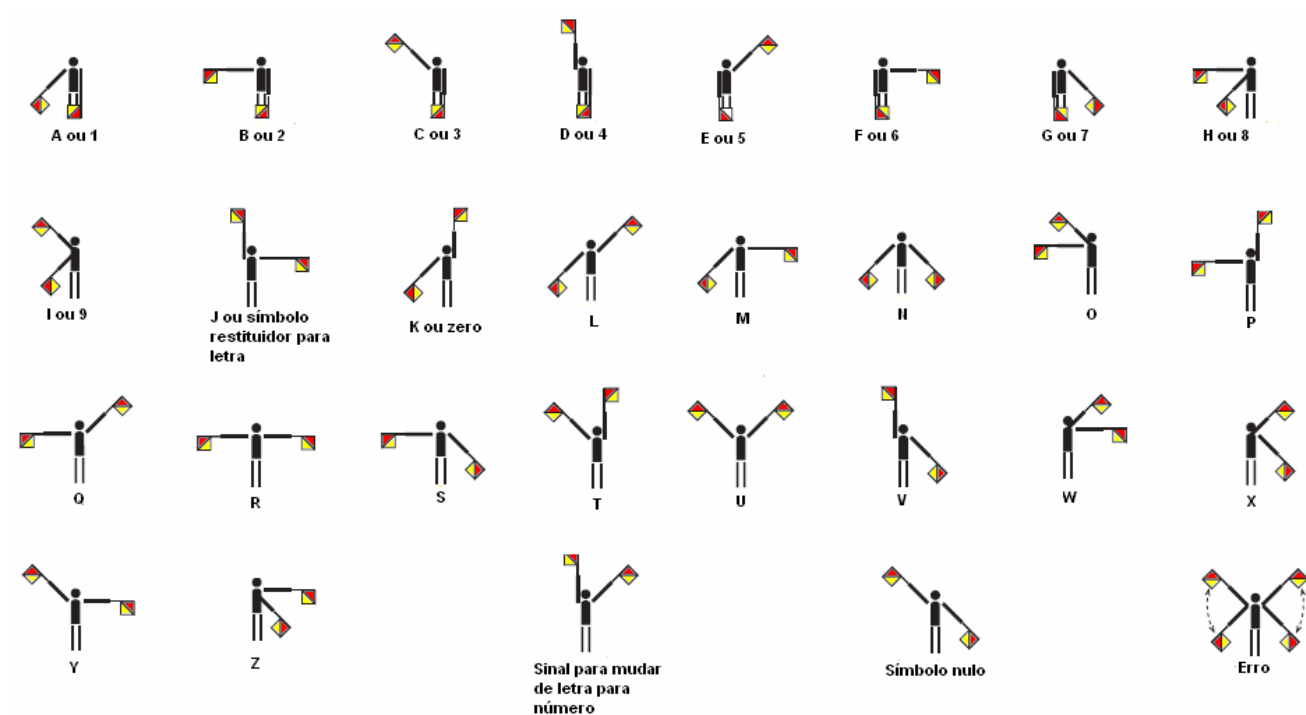
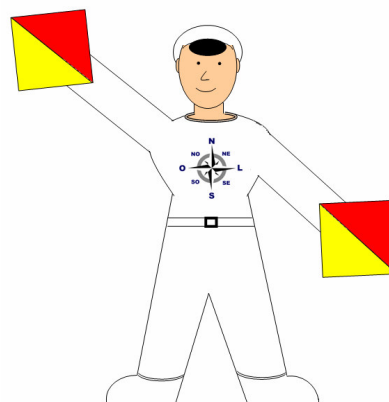
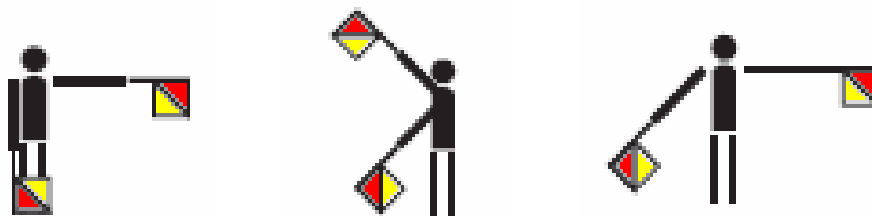
Entregue o cadeado mágico para alguém que queira abri-lo.

COMUNICAÇÃO COM BANDEIRINHAS:

A ou 1 | B ou 2 | C ou 3 | D ou 4 | E ou 5 | F ou 6 | G ou 7 | H ou 8

I ou 9 | J ou símbolo restituidor para letra | K ou zero | L | M | N | O | P

Q | R | S | T | U | V | W | X

Y | Z | Sinal para mudar de letra para número | Símbolo nulo | Erro

Aqui nos despedimos, desejando que tenham tido uma boa diversão e uma boa aprendizagem!

REFERÊNCIAS

BERLOQUIN, P., **100 jogos numéricos e 100 jogos lógicos**, RBA , 208.

FOLHA DE SÂO PAULO -20/07010 Caderno Fovest

FOLHINHA DE SÃO PAULO (jornal FSP 26/04/03)

GARDNER, Martin **6th Book of Mathematical Diversions from Scientific American**.

MALAGUTTI, P. L. **Atividades de Contagem a Partir da Criptografia.** Disponível em http: //www.obmep.org.br. Acessado em 26/07/2010.

MORGADO, PITOMBEIRA, CARVALHO, FERNANDEZ, **Análise Combinatória e Probabilidade** IMPA, 1991.

SGARRO, A. **Códigos Secretos: Criptografia.** Editora Melhoramentos: São Paulo,1989.

Bletchley Park Site: http://www.bletchleypark.org.uk/. Acessado em 26/07/2010.

http://paper-replika.com/index.php?option=com_content&view=article&id=527:german-m4-naval-enigma-machine&catid=38&Itemid=200920
senha: paper-replika.com, acessado em 21/07/2010.

http://mckoss.com/Crypto/Paper%20Enigma.pdf

http://www.cimt.plymouth.ac.uk/resources/codes/default.htm, acessado em 21/07/2010.

http://www.ibc.gov.br/?catid=110&blogid=1&itemid=479, acessado em 21/07/2010.